2639 - 1264

1916-1917

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

EDITED BY

ORMOND STONE
L. P. EISENHART
OSWALD VEBLEN
PIERRE BOUTROUX
T. H. GRONWALL
J. H. M. WEDDERBURN

WITH THE COÖPERATION OF

J. W. ALEXANDER
R. D. CARMICHAEL
A. A. BENNETT
H. H. MITCHELL

PUBLISHED UNDER THE AUSPICES OF PRINCETON UNIVERSITY

LIBRARY
LELAND STANFORD JUNIOR
UNIVERSITY

SECOND SERIES VOL. 18

LANCASTER, PA., AND PRINCETON, N. J.

LIBRARY
LELAND STANFORD JUNIOR
UNIVERSITY

ON THE SURFACE OF LOWEST DEGREE PASSING THROUGH A GIVEN CURVE IN SPACE.

By Tsuruichi Hayashi.

1. For the classification of curves in space, it is necessary to determine the lowest degree of the surfaces which contain a given curve.* For that purpose Salmon made use of the principle that a curve of degree m meets a surface of degree k in mk points, and many other investigators followed him. From this principle it follows that if we take on a curve of degree m as many points as are sufficient to determine a surface of degree k, and if the number of points so assumed be greater than mk, the surface described through the points must altogether contain the curve, for otherwise the principle would be violated.

Since the number of points through which a surface of degree k can be drawn is

$$\frac{k(k^2+6k+11)}{6} = \varphi(k) \text{ say,}$$

when $\varphi(k) = mk+1$, one and only one surface of degree k contains the given curve of degree m, and when $\varphi(k) > mk+1$, two surfaces of degree k can be drawn, and therefore an infinite number.

If one or two surfaces of degree k contain the curve, two surfaces and therefore an infinite number of surfaces of degree higher than k contain the curve. For, if $\varphi(k) \geqq mk+1$, then

$$\begin{aligned}\varphi(k+n) - m(k+n) - 1 &> \frac{(k+n)(k+n^2+6k+n+11)}{6} - \frac{k^2+6k+11}{6}(k+n) - 1 \\ &> \frac{n(k+n)}{6}(2k+n+6) - 1 > 0,\end{aligned}$$

so that $\varphi(k+n) > m(k+n) - 1$.

2. Now let us proceed to discuss the equation $\varphi(k) = mk+1$, which may be written

$$k^2+6k+11 = 6m + \frac{6}{k}.$$

* As my discussion is general, the word "general" should be used in speaking of curve and surface, thus "general curve" and "general surface." But for the sake of brevity I omit the word throughout.

Evidently $k = 1, 2, 3$ or 6. The last possibility does not give an integral value for m. Hence the only possibilities are

$$k = 1,\ m = 2; \qquad k = 2,\ m = 4; \qquad k = 3,\ m = 6.$$

The first case, that of a conic with a plane through it, is trivial. The other results may be stated thus:

Through the general quartic curve there passes a quadric surface, and through the general sextic a cubic surface.

We shall consider these two cases further.

In these two cases only, one and only one proper surface of degree k can be drawn containing the given curve in space. Two and only two classes of curves, quartic and sextic, can be divided into two families respectively, so that through a given curve belonging to the first family two and therefore more surfaces can be drawn, while through one belonging to the second family one and only one surface can be drawn. Remarks are necessary when the surfaces are not proper. For example, there are three kinds of quartic curves determined by a plane and a quartic surface, by two quadric surfaces, and by a quadric surface and a cubic surface; through any quartic curve of the first and second kinds, two and more quadric surfaces can be drawn, those for the first kind being improper quadrics, viz., quadrics resolved into two planes, one of which is fixed and the other is arbitrary; and through any quartic curve of the third kind, one and only one quadric surface can be drawn. There are two kinds of quintic curves determined by a quadric surface and a cubic surface, and by two cubic surfaces; through any quintic curve of either kind we can draw two and therefore more cubic surfaces. There are three kinds of sextic curves determined by a quadric surface and a cubic surface, by two cubic surfaces, and by a cubic surface and a quartic surface; through any sextic curve of the first and second kinds two and more cubic surfaces can be drawn, while through any one of the third kind one and only one cubic surface can be drawn. The other classes of curves, septic and of the higher degree, can not be divided into such two families. Through all of them we can draw two and therefore an infinite number of surfaces of a certain degree. That degree is given by the smallest value of k satisfying the inequality

$$\varphi(k) > mk + 1$$

for a given value of m.

3. Now let us find this smallest value of k. This inequality becomes

$$f(k) \equiv k^3 + 6k^2 - (6m - 11)k - 6 > 0.$$

If we put $k + 2 = \bar{k}$, the equation $f(k) = 0$ is reducible to the canonical form

$$\bar{k}^3 - (6m + 1)\bar{k} + 12(m - 1) = 0.$$

As the discriminant of this equation, namely

$$\left(\frac{12(m-1)}{2}\right)^2 - \left(\frac{6m+1}{3}\right)^3,$$

is negative for $m \geqq 2$, the three roots are real and distinct.

Applying the method of trigonometric solution of this irreducible cubic, we have that the three roots are

$$2\sqrt{\frac{6m+1}{3}}\cos\frac{\alpha}{3}, \qquad 2\sqrt{\frac{6m+1}{3}}\cos\frac{2\pi-\alpha}{3}, \qquad 2\sqrt{\frac{6m+1}{3}}\cos\frac{2\pi+\alpha}{3},$$

where α is the least positive value given by

$$\cos\alpha = -6(m-1)\sqrt{\frac{27}{(6m+1)^3}},$$

the radicals indicating the positive square roots.

Since $m \geqq 2$, $\pi/2 < \alpha < \pi$. Hence the first two of the above roots are positive and the third is negative. Moreover, the first is the larger of the positive roots. Therefore

Two and more surfaces of degree k can be drawn through the given curve of degree m, if k be selected not less than k_1, for which the relation

$$k_1 = 2\sqrt{\frac{6m+1}{3}}\cos\frac{\alpha}{3} - 2$$

holds, α being the least positive value satisfying

$$\cos\alpha = -6(m-1)\sqrt{\frac{27}{(6m+1)^3}}.$$

This gives the exact values of the greatest suffixes of the left A's in Halphen's tables in his memoir *Sur la classification des courbes gauches algébriques*, Journal de l'École Polytéchnique, vol. 52, 1882 [pp. 1–200], pp. 161–186.

SENDAI, JAPAN,
February, 1915.

A PRACTICAL METHOD OF DETERMINING ELEMENTARY DIVISORS.

By H. T. Burgess.

So far as the writer of this brief paper is aware, no method is known for determining the elementary divisors of a given matrix $\lambda A + B$ which does not involve an extremely large amount of labor.*

It is the object of this paper to give a method which is both simple and practical. The few well-known theorems on which it is based will be stated without proof.

I. Characteristic Matrices.

Fundamental Theorem.—Let $\lambda I + B$ be any characteristic matrix whose characteristic equation is

$$\varphi(\lambda) = (\lambda - \alpha_1)^{t_1}(\lambda - \alpha_2)^{t_2} \cdots (\lambda - \alpha_s)^{t_s} \cdots (\lambda - \alpha_\eta)^{t_\eta} = 0.$$

There exists a similar characteristic matrix $\lambda I + N$ with the same elementary divisors. It is of the normal form

$$\lambda I + N = \begin{vmatrix} \lambda I + N_{t_1} & & & & \\ & \lambda I + N_{t_2} & & & \\ & & \cdots & & \\ & & & \lambda I + N_{t_s} & \\ & & & & \cdots \\ & & & & \lambda I + N_{t_\eta} \end{vmatrix},$$

in which all elements are zero except those in the non-overlapping principal minors indicated. Any one of these principal minors as $\lambda I + N_{t_s}$ is a characteristic matrix of order t_s and has the form

$$\lambda I + N_{t_s} = \begin{vmatrix} \lambda I + E_{e_1} & & & & \\ & \lambda I + E_{e_2} & & & \\ & & \cdots & & \\ & & & \lambda I + E_{e_\pi} & \\ & & & & \cdots \\ & & & & \lambda I + E_{e_\tau} \end{vmatrix},$$

in which all elements are zero except those in the non-overlapping principal minors indicated. Any one of these principal minors as $\lambda I + E_{e_\pi}$ is of order e_π and has all of its elements zero except in its principal and over-principal diagonals, all of the elements in the principal diagonal being

* Bôcher, Introduction to Higher Algebra, p. 272.

equal to $\lambda - \alpha_\epsilon$ and all of the elements in the over-principal diagonal, to one. Further we have the relation

$$e_1 \geqq e_2 \geqq \cdots \geqq e_\pi \geqq \cdots \geqq e_\tau$$

and these e's are the exponents of the elementary divisors of $\lambda I + B$ or $\lambda I + N$ which are connected with the linear factor $\lambda - \alpha_\epsilon$.*

THEOREM 1. If n is a positive integer, the matrices $(\lambda I + B)^n$ and $(\lambda I + N)^n$, where $\lambda I + B$ and $\lambda I + N$ are similar, have the same ranks.

If $\lambda I + B$ and $\lambda I + N$ are similar, there exists a non-singular matrix H such that

$$H^{-1}(\lambda I + B)H = \lambda I + N.$$

Hence

$$H^{-1}(\lambda I + B)^n H = (\lambda I + N)^n,$$

for

$$H^{-1}(\lambda I + B)^n H = H^{-1}(\lambda I + B)H \cdot H^{-1}(\lambda I + B)H \cdot \cdots \text{ to } n \text{ factors.}$$

THEOREM 2. Let $r_1, r_2, \cdots$ be the ranks of $(\alpha_\epsilon I + B)^n$ for $n = 1, 2, \cdots$; then the exponents of the elementary divisors of $\lambda I + B$ which are connected with the linear factor $\lambda - \alpha_\epsilon$ are uniquely determined by the following table:

$m - r_\kappa$	e_1	e_2	$\cdots$	e_π	$\cdots$	e_τ
$r_1 - r_\kappa$	$e_1 - 1$	$e_2 - 1$	$\cdots$	$e_\pi - 1$	$\cdots$	$e_\tau - 1$
$r_2 - r_\kappa$	$e_1 - 2$	$e_2 - 2$	$\cdots$	$e_\pi - 2$	$\cdots$	$e_\tau - 2$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

which is completely defined as follows: The order of $\lambda I + B$ is m and

I. There are κ rows where $r_1 > r_2 > r_3 > \cdots > r_{\kappa-1} > r_\kappa = r_{\kappa+1}$.

II. In any row the sum of the integers appearing is equal to the number at the left end of that row.

III. In the bottom row the integers appearing are all ones and are at the left $r_{\kappa-1} - r_\kappa$ in number. The spaces to the right are blank.

IV. In each successive row from the bottom upward each integer is one greater than that directly beneath it and a sufficient number of ones appear on the right to satisfy II.

Proof. By Theorem 1, the ranks $r_1, r_2, \cdots r_\kappa$ are the same for $(\alpha_\epsilon I + N)^n$. By the laws of matrix multiplication, it appears that $(\alpha_\epsilon I + N)^n$ is immediately obtained by writing $(\alpha_\epsilon I + N_{t_\epsilon})^n$ in place of $\alpha_\epsilon I + N_{t_\epsilon}$ in $\alpha_\epsilon I + N$ for $\epsilon = 1, 2, \cdots \eta$. In like manner $(\alpha_\epsilon I + N_{t_\epsilon})^n$ is obtained by writing $(\alpha_\epsilon I + E_{e_\pi})^n$ in place of $\alpha_\epsilon I + E_{e_\pi}$ in $\alpha_\epsilon I + N_{t_\epsilon}$

* A complete and direct demonstration of this theorem is given by H. E. Hawkes in the American Journal of Mathematics, vol. XXXII, No. 2, pp. 101–109.

for $\pi = 1, 2, \cdots \tau$. Inspection of these results shows that the rank of $(\alpha_\epsilon I + N)^n$ is the sum of the ranks of its non-overlapping principal minors and that the same is true of $(\alpha_\epsilon I + N_{t_\epsilon})^n$. Further it is obvious that the sum of the ranks of all of the principal minors of $(\alpha_\epsilon I + N)^n$ excepting $(\alpha_\epsilon I + N_{t_\epsilon})^n$ is $m - t_\epsilon$; for their ranks do not change with n. Again if we compute $(\alpha_\epsilon I + E_{e_\pi})^n$, we see that, for $n = 1, 2, \cdots e_{\pi-1}, e_\pi$, the ranks are $e_\pi - 1, e_\pi - 2, \cdots 1, 0$. Since the ranks of these principal minors in $(\alpha_\epsilon I + N_{t_\epsilon})^n$ become zero as n increases through the succession $e_\tau \cdots e_\pi \cdots e_2, e_1$, we have $r_\kappa = m - t_\epsilon$ and $\kappa = e_1$. This establishes the theorem.

Illustration. Suppose we have a characteristic matrix of order 10 whose characteristic equation has $\lambda - \alpha$ as a linear factor, and that for this root α the ranks of $(\alpha I + B)^n$ are $r_1 = 6, r_2 = 4, r_3 = 3, r_4 = 3$; then $\kappa = 3$ and the table is

$$\begin{array}{ccccc} 7 & 3 & 2 & 1 & 1 \\ 3 & 2 & 1 & & \\ 1 & 1 & & & \end{array}$$

It thus appears that we need only to know the successive ranks $r_1 > r_2 > \cdots > r_{\kappa-1} > r_\kappa = r_{\kappa+1}$ of $(\alpha I + B)^n$ for $n = 1, 2, \cdots, \kappa - 1, \kappa, \kappa + 1$ in order to compute the exponents of the elementary divisors associated with the linear factor $\lambda - \alpha$. That this method is exceedingly simple in comparison with the ordinary method is apparent.

II. Matrices of the type $\lambda_1 A + \lambda_2 B$.

Case 1. If A is non-singular, we know that $\lambda_1 I + \lambda_2 A^{-1}B$ has the same elementary divisors as $\lambda_1 A + \lambda_2 B$.* Hence we determine the elementary divisors for the characteristic matrix $\lambda I + A^{-1}B$.

Case 2. If A and B are both singular, but $|\lambda_1 A + \lambda_2 B| \neq 0$ identically in λ_1 and λ_2, the method is applicable. All that is necessary is to transform the parameters by a non-singular linear transformation in such a manner that the resulting matrix $\lambda_1' A' + \lambda_2' B'$ is brought under case 1. The exponents of the elementary divisors will be the same and the corresponding linear factors will be connected by the transformation of the parameters.†

Case 3. In case $|\lambda_1 A + \lambda_2 B| = 0$ identically in λ_1 and λ_2, the method can be applied provided the matrix can be reduced by elementary transformations to an equivalent matrix of lower order which falls under case 2.

UNIVERSITY OF WISCONSIN,
MADISON, WISCONSIN.

* Bôcher, Introduction to Higher Algebra, section 94.

† Muth, Elementarteiler, p. 63.

CONJUGATE SYSTEMS WITH EQUAL POINT INVARIANTS.

By Luther Pfahler Eisenhart.

When the developables of a rectilinear congruence meet a surface S in a conjugate system of curves, the conjugate system and the congruence are said to be *conjugate* to one another. When the conjugate system on S is parametric, its point coördinates satisfy a partial differential equation of the Laplace type. Each solution μ of the adjoint differential equation determines a congruence conjugate to the given system. Each solution θ of the point equation of S determines a new conjugate system S_1 conjugate to this congruence. We say that S_1 is obtained from S by a *transformation* $T(\mu, \theta)$.

The interrelations of S and S_1 with their Laplace transforms S^{-1}, S' and S_1^{-1}, S_1' are studied. The tangent planes to S osculate one family of curves on S^{-1} and the other family on S'. Accordingly there is a pencil of conics each of which is tangent to these curves at corresponding points. There exist similar pencils of conics in the tangent planes to S_1. We show that the pencils in corresponding planes cut out on the intersection of these planes the same involution only in case the point equation of S has equal invariants and also that of S_1. We have thus a characteristic property of the transformations K.* In this case the conics of the two pencils are paired, so that those of a pair meet and determine a pencil of quadrics. Certain properties of these pencils of quadrics are determined. It is shown also that each congruence conjugate to a conjugate system with equal point invariants leads at once to a transformation K. This result is useful, in particular, in the determination of surfaces Ω.† Throughout the paper homogeneous coördinates are used, and the results are projective.

1. Transformations $T(\mu, \theta)$.

The necessary and sufficient condition that four functions x, y, z, w be the homogeneous point coördinates of a surface S referred to a conjugate system of parameters u and v is that these functions satisfy an equation of the form

$$\frac{\partial^2\theta}{\partial u \partial v} + a\frac{\partial\theta}{\partial u} + b\frac{\partial\theta}{\partial v} + c\theta = 0, \tag{1}$$

* Transactions of the American Mathematical Society, vol. 15 (1914), pp. 397–430.

† Transactions of the American Mathematical Society, vol. 16 (1915), pp. 275–310.

where a, b, c are functions of u and v. We refer to this equation as the point equation of the conjugate system.

Darboux* has shown that when a solution μ of the equation adjoint to (1), namely

$$\frac{\partial^2\mu}{\partial u\partial v} - a\frac{\partial\mu}{\partial u} - b\frac{\partial\mu}{\partial v} + \left(c - \frac{\partial a}{\partial u} - \frac{\partial b}{\partial v}\right)\mu = 0, \tag{2}$$

is known, a congruence conjugate to the given conjugate system is given by quadratures. In fact, the coördinates X_1, Y_1, Z_1, W_1; X_2, Y_2, Z_2, W_2, of the focal points F_1 and F_2 of this congruence are given by equations of the form

$$\begin{aligned} X_1 &= \int\left[\mu\left(\frac{\partial x}{\partial u} + bx\right)du + x\left(\frac{\partial\mu}{\partial v} - a\mu\right)dv\right], \\ X_2 &= \int\left[x\left(\frac{\partial\mu}{\partial u} - b\mu\right)du + \mu\left(\frac{\partial x}{\partial v} + ax\right)dv\right]. \end{aligned} \tag{3}$$

Each solution θ of (1), linearly independent of x, y, z, w, leads by quadratures to a conjugate system conjugate to the above congruence. In fact, if μ is the function appearing in (3) and θ is such a solution of (1), the function σ given by

$$\sigma = \int\left[\mu\left(\frac{\partial\theta}{\partial u} + b\theta\right)du + \theta\left(\frac{\partial\mu}{\partial v} - a\mu\right)dv\right] \tag{4}$$

is a solution of the point equation of (F_1), the locus of F_1, and is linearly independent of X_1, Y_1, Z_1, W_1. Hence by the theorem of Levy† the surface S_1, whose coördinates x_1, y_1, z_1, w_1 are given by equations of the form

$$x_1 = X_1 - \frac{\sigma}{\dfrac{\partial\sigma}{\partial v}}\frac{\partial X_1}{\partial v} = X_1 - \frac{\sigma x}{\theta}, \tag{5}$$

is conjugate to the congruence whose focal surfaces are (F_1) and (F_2). We say that the new conjugate system is obtained from the original one by a *transformation* $T(\mu, \theta)$.

If μ is held fixed, and θ is any solution of (1), we get all the conjugate systems conjugate to this congruence. Hence equations (3), (4) and (5) define the general transformation $T(\mu, \theta)$.

From (5) we find at once

$$\frac{\partial x_1}{\partial u} = (\mu\theta - \sigma)\frac{\partial}{\partial u}\left(\frac{x}{\theta}\right), \qquad \frac{\partial x_1}{\partial v} = -\sigma\frac{\partial}{\partial v}\left(\frac{x}{\theta}\right). \tag{6}$$

* Leçons, vol 2, p. 225.

† Journal de l'Ecole Polytechnique, cahier 56 (1886), p. 63; also Darboux, Leçons, vol. 2, p. 222.

From these equations we see that the points $T_1(\xi_1, \eta_1, \zeta_1, \omega_1)$, $T_2(\xi_2, \eta_2, \zeta_2, \omega_2)$, whose coördinates are given by equations of the form

$$\xi_1 = \theta \frac{\partial x}{\partial u} - x \frac{\partial \theta}{\partial u}, \qquad \xi_2 = \theta \frac{\partial x}{\partial v} - x \frac{\partial \theta}{\partial v}, \tag{7}$$

are the points of intersection of the tangents to the curves v = const. and the curves u = const. respectively on S and S_1.

By differentiation we find

$$\begin{aligned} \frac{\partial \xi_1}{\partial v} &= \left(\frac{\partial \log \theta}{\partial v} - a \right) \xi_1 - \left(\frac{\partial \log \theta}{\partial u} + b \right) \xi_2, \\ \frac{\partial \xi_2}{\partial u} &= -\left(\frac{\partial \log \theta}{\partial v} + a \right) \xi_1 + \left(\frac{\partial \log \theta}{\partial u} - b \right) \xi_2. \end{aligned} \tag{8}$$

Consequently T_1 and T_2 are the focal points of the congruence of lines T_1T_2.

The equations of S_1 can be given another form, if we look upon the lines of the given congruence as tangent to the focal surface (F_2) also. Evidently the function τ, given by

$$\tau = \int \left[\theta \left(\frac{\partial \mu}{\partial u} - b\mu \right) du + \mu \left(\frac{\partial \theta}{\partial v} + a\theta \right) dv \right], \tag{4'}$$

is a solution of the point equation of (F_2). The equations of S_1 are of the form

$$x_1 = -X_2 + \frac{\tau x}{\theta}, \tag{5'}$$

and we have also

$$\frac{\partial x_1}{\partial u} = \tau \frac{\partial}{\partial u}\left(\frac{x}{\theta} \right), \qquad \frac{\partial x_1}{\partial v} = -(\mu\theta - \tau) \frac{\partial}{\partial v}\left(\frac{x}{\theta} \right). \tag{6'}$$

It is readily shown that these equations are consistent with (5) and (6), if we take

$$\tau = \mu\theta - \sigma, \tag{9}$$

which is consistent also with (4) and (4').

2. Transformations of Laplace of S and S_1.

If lines be drawn tangent to the curves v = const. on S, we get a congruence one of whose focal surfaces is S, and the other focal surface S^{-1}, called a *Laplace transform* of S, is defined by equations of the form

$$x^{-1} = \frac{\partial x}{\partial u} + bx, \tag{10}$$

and similar expressions for the other coördinates y^{-1}, z^{-1}, w^{-1} of the point M^{-1}.* In like manner the coördinates x', y', z', w' of M', the corresponding point on the other Laplace transform, obtained by drawing the tangents to the curves $u = \text{const.}$ on S, are of the form

$$x' = \frac{\partial x}{\partial v} + ax. \tag{11}$$

From (6) we derive the point equation of S_1, namely

$$\frac{\partial^2 \theta_1}{\partial u \partial v} + a_1 \frac{\partial \theta_1}{\partial u} + b_1 \frac{\partial \theta_1}{\partial v} = 0, \tag{12}$$

where

$$a_1 = \frac{\sigma\left(a + \dfrac{\partial \log \theta}{\partial v}\right)}{\sigma - \mu\theta}, \qquad b_1 = \frac{\sigma - \mu\theta}{\sigma}\left(b + \frac{\partial \log \theta}{\partial u}\right). \tag{12'}$$

The equations of the Laplace transforms S_1^{-1} and S_1' of S_1 are analogous to (10) and (11). By means of (5), (5'), (6), (6'), (9) and (12') these are reducible to

$$\begin{aligned} x_1^{-1} &= \frac{\partial x_1}{\partial u} + b_1 x_1 = b_1 X_1 + \frac{\mu\theta - \sigma}{\theta} x^{-1}, \\ x_1' &= \frac{\partial x_1}{\partial v} + a_1 x_1 = -a_1 X_2 + \frac{\tau - \mu\theta}{\theta} x'. \end{aligned} \tag{13}$$

From (3), (10) and (11) we have

$$\frac{\partial X_1}{\partial u} = \mu x^{-1}, \qquad \frac{\partial X_2}{\partial v} = \mu x'. \tag{14}$$

Comparing these results, we have

THEOREM 1. *Corresponding points on S^{-1} and S_1^{-1} lie on the corresponding tangent to the curve $v = \text{const.}$ on (F_1); corresponding points on S' and S_1' lie on the corresponding tangent to the curve $u = \text{const.}$ on (F_2).*

3. Pencils of conics in the tangent planes to S and S_1.

In order to study certain configurations associated with transformations $T(\mu, \theta)$, we take for tetrahedron of reference $MM_1T_1T_2$, where M and M_1 are corresponding points on S and S_1, and T_1 and T_2 are given by (7). If we take

$$M(0, 1, 0, 1), \qquad M_1(0, 0, 0, 1), \qquad T_1(1, 0, 0, 0), \qquad T_2(0, 0, 1, 0),$$

we have from (6) and (7)

* Darboux, Leçons, vol. 2, p. 19.

$$\frac{\partial x}{\partial u} = \frac{1}{\theta}, \qquad \frac{\partial y}{\partial u} = \frac{\partial \log \theta}{\partial u}, \qquad \frac{\partial z}{\partial u} = \frac{\partial w}{\partial u} = 0,$$

$$\frac{\partial x}{\partial v} = 0, \qquad \frac{\partial y}{\partial v} = \frac{\partial \log \theta}{\partial v}, \qquad \frac{\partial z}{\partial v} = \frac{1}{\theta}, \qquad \frac{\partial w}{\partial v} = 0.$$

Hence from (10) and (11) follow

$$x^{-1} = \frac{1}{\theta}, \qquad y^{-1} = \frac{\partial \log \theta}{\partial u} + b, \qquad z^{-1} = w^{-1} = 0,$$

$$x' = 0, \qquad y' = \frac{\partial \log \theta}{\partial v} + a, \qquad z' = \frac{1}{\theta}, \qquad w' = 0.$$

We have denoted by M^{-1} and M' the points with these coördinates.

The pencil of conics in the tangent plane to S at M tangent to MM^{-1} and MM' at M^{-1} and M' is given by

$$2\lambda xz = \left[\left(\frac{\partial \log \theta}{\partial u} + b\right)x - \frac{y}{\theta} + \left(\frac{\partial \log \theta}{\partial v} + a\right)z\right]^2. \tag{15}$$

From the theory of congruences it follows that the tangent plane at M is the osculating plane of the curve $u = \text{const.}$ on S^{-1} at M^{-1}. We seek λ so that the above equation shall give a conic osculating $u = \text{const.}$ at this point. The necessary and sufficient condition is that the above equation shall be satisfied to within terms of the second order in dv by expressions of the form

$$x^{-1} + \frac{\partial x^{-1}}{\partial v}\,dv + \frac{1}{2}\frac{\partial^2 x^{-1}}{\partial v^2}\,dv^2.$$

From (10) we have in general

$$\frac{\partial x^{-1}}{\partial v} = -a\frac{\partial x}{\partial u} + \left(\frac{\partial b}{\partial v} - c\right)x, \qquad \frac{\partial^2 x^{-1}}{\partial v^2} = A\frac{\partial x}{\partial u} + k\frac{\partial x}{\partial v} + Bx,$$

where

$$A = a^2 - \frac{\partial a}{\partial v}, \qquad k = \frac{\partial b}{\partial v} + ab - c, \qquad B = ac + \frac{\partial^2 b}{\partial v^2} - \frac{\partial c}{\partial v}. \tag{16}$$

For the present choice of tetrahedron we have

$$\frac{\partial x^{-1}}{\partial v} = -\frac{a}{\theta}, \qquad \frac{\partial y^{-1}}{\partial v} = -a\frac{\partial \log \theta}{\partial u} + \frac{\partial b}{\partial v} - c, \qquad \frac{\partial z^{-1}}{\partial v} = \frac{\partial w^{-1}}{\partial v} = 0,$$

$$\frac{\partial^2 x^{-1}}{\partial v^2} = \frac{A}{\theta}, \qquad \frac{\partial^2 y^{-1}}{\partial v^2} = A\frac{\partial \log \theta}{\partial u} + k\frac{\partial \log \theta}{\partial v} + B,$$

$$\frac{\partial^2 z^{-1}}{\partial v^2} = \frac{k}{\theta}, \qquad \frac{\partial^2 w^{-1}}{\partial v^2} = 0.$$

Making use of these values, we find that in the pencil of conics (15) the osculating conic of $u = \text{const.}$ is given by $\lambda = k$.

Proceeding in like manner, we find that, when

$$\lambda = h = \frac{\partial a}{\partial u} + ab - c, \tag{17}$$

the corresponding conic of the pencil (15) osculates the curve $v = \text{const.}$ at M'.

The functions h and k, defined by (17) and (16) are the invariants of equation (1). A consequence of the above results is the theorem of Koenigs:

THEOREM 2. *A necessary and sufficient condition that there exist a conic of the pencil* (15) *osculating the curves* $u = \text{const.}$ *on* S^{-1} *and* $v = \text{const.}$ *on* S' *is that the invariants of equation* (1) *be equal.*

By the same sort of processes and with the aid of the foregoing formulas we can show that the conics in the tangent plane to S_1 at M_1 and tangent at M_1^{-1} and M_1' to the lines $M_1M_1^{-1}$ and M_1M_1' respectively are defined by

$$2xz = \lambda_1\left[\frac{x}{\sigma}\left(b + \frac{\partial \log \theta}{\partial u}\right) - \frac{z}{\tau}\left(a + \frac{\partial \log \theta}{\partial v}\right) + \frac{w}{\theta^2}\right]^2. \tag{18}$$

When $-\sigma\tau/\lambda_1$ is equal to k_1 or h_1, the invariants of (12), the corresponding conics osculate the curves $u = \text{const.}$ on S_1^{-1} or $v = \text{const.}$ on S_1'.

Each of the pencils of conics (15) and (18) determines an involution on the line T_1T_2 ($y = w = 0$), and the points T_1, T_2 are a conjugate pair in each involution. In order that these involutions be identical, it is necessary and sufficient that they have another conjugate pair in common. From equations (15) and (18) it is seen that a necessary condition for this is

$$\sigma^2 = \tau^2.$$

Since $\mu \neq 0$, $\theta \neq 0$, we have from (9)

$$\sigma = \tau = \tfrac{1}{2}\mu\theta.$$

In order that this value may satisfy (4), we must have

$$\frac{\partial}{\partial u}\log\sqrt{\frac{\mu}{\theta}} = b, \qquad \frac{\partial}{\partial v}\log\sqrt{\frac{\mu}{\theta}} = a. \tag{19}$$

The consistency of these equations requires that the invariants h and k of equation (1) shall be equal.

4. Transformations K. Osculating conics.

We consider now the case where $h = k$, and are take equation (1) in the form

$$\frac{\partial^2\theta}{\partial u\partial v}+\frac{\partial \log \sqrt{\rho}}{\partial v}\frac{\partial\theta}{\partial u}+\frac{\partial \log \sqrt{\rho}}{\partial u}\frac{\partial\theta}{\partial v}+c\theta=0. \tag{20}$$

The invariants of this equation have the value

$$h=k=\frac{\partial^2 \log \sqrt{\rho}}{\partial u\partial v}+\frac{\partial \log \sqrt{\rho}}{\partial u}\frac{\partial \log \sqrt{\rho}}{\partial v}-c. \tag{21}$$

By choosing suitably the constant of integration in (19), we have

$$\mu=2\rho\theta, \qquad \sigma=\rho\theta^2.$$

It is readily shown that this value of μ satisfies the equation adjoint to (20).

The corresponding equations (6) are

$$\frac{\partial x_1}{\partial u}=\rho\theta^2\frac{\partial}{\partial u}\left(\frac{x}{\theta}\right), \qquad \frac{\partial x_1}{\partial v}=-\rho\theta^2\frac{\partial}{\partial v}\left(\frac{x}{\theta}\right). \tag{22}$$

The point equation of S_1 is

$$\frac{\partial^2\theta_1}{\partial u\partial v}-\frac{\partial}{\partial v}\log\theta\sqrt{\rho}\frac{\partial\theta_1}{\partial u}-\frac{\partial}{\partial u}\log\theta\sqrt{\rho}\frac{\partial\theta_1}{\partial v}=0, \tag{23}$$

so that its invariants are equal and are given by

$$h_1=k_1=2\frac{\partial \log \sqrt{\rho\theta}}{\partial u}\frac{\partial \log \sqrt{\rho\theta}}{\partial v}-h. \tag{24}$$

From (5) and (5′) it follows that the coördinates of the focal points of the congruence of joins of corresponding points M and M_1 on S and S_1 are of the form

$$X_1=x_1+\rho\theta x, \qquad X_2=-x_1+\rho\theta x. \tag{25}$$

Hence the focal points are harmonic to M and M_1, and we have

THEOREM 3. *When equation* (1) *has equal invariants, to each solution* θ *there corresponds a transformation* $T(2\rho\theta, \theta)$ *such that on* S_1 *the parametric conjugate system has equal invariants, and the focal points of the lines joining corresponding points on* S *and* S_1 *are harmonic to the latter points.*

Accordingly equations (22) define in homogeneous coördinates the transformation K which we have considered at length elsewhere.* In fact, if the homogeneous coördinates are rectangular so that $w=1$, then $c=0$. Now w_1 is given by

$$\frac{\partial w_1}{\partial u}=-\rho\frac{\partial\theta}{\partial u}, \qquad \frac{\partial w_1}{\partial v}=\rho\frac{\partial\theta}{\partial v}. \tag{26}$$

* Transactions, l. c.

Hence the rectangular non-homogeneous coördinates x_1, y_1, z_1 of S_1 are given by

$$(27)\quad \frac{\partial}{\partial u}(x_1 w_1) = -\rho\left(x\frac{\partial\theta}{\partial u} - \theta\frac{\partial x}{\partial u}\right), \qquad \frac{\partial}{\partial v}(x_1 w_1) = \rho\left(x\frac{\partial\theta}{\partial v} - \theta\frac{\partial x}{\partial v}\right),$$

which are the same as the equations previously obtained.

In the case of a transformation K the equations (15) and (18) are reducible to

$$(28)\quad 2exz = \left(\frac{\partial \log \theta\sqrt{\rho}}{\partial u}x - \frac{y}{\theta} + \frac{\partial \log \theta\sqrt{\rho}}{\partial v}z\right)^2,$$

$$(29)\quad 2fxz = \left(\frac{\partial \log \theta\sqrt{\rho}}{\partial u}x - \frac{\partial \log \theta\sqrt{\rho}}{\partial v}z + \rho w\right)^2,$$

where e and f are the parameters of these pencils of conics. The necessary and sufficient condition that a conic of each pencil meet on $y = w = 0$ is that the parameters satisfy the equation

$$(30)\quad f = e - 2\frac{\partial \log \sqrt{\rho}\theta}{\partial u}\cdot\frac{\partial \log \sqrt{\rho}\theta}{\partial v}.$$

From (17) it follows that when $e = h = k$, the conic osculates the curve $u = \text{const.}$ on S^{-1} at M^{-1} and the curve $v = \text{const.}$ on S' at M'. We call the conic C_0. We obtain the analogous conic C_{10}, osculating the respective curves on S_1^{-1} and S_1^{1} by putting in (29) $f = -h_1 = -k_1$. In consequence of (24) these values of e and f satisfy (30). Hence the conics C_0 and C_{10} meet on the line $y = w = 0$, and we have

THEOREM 4. *When S and S_1 are two surfaces in the relation of a transformation K, the pencils of conics* (15) *and* (18) *determine the same involution on the line of intersection of the tangent planes to S and S_1; in particular the osculating conics C_0 and C_{10} meet on this line.**

Consider two conics of the pencils (28) and (29) whose parameters satisfy the condition (30). Through these two conics there pass a pencil of quadrics, whose equation is

$$(31)\quad \begin{aligned}&\left(\frac{\partial \log \sqrt{\rho}\theta}{\partial u}\right)^2 x^2 + \frac{y^2}{\theta^2} + \left(\frac{\partial \log \sqrt{\rho}\theta}{\partial v}\right)^2 z^2 + \rho^2 w^2 - \frac{2}{\theta}\frac{\partial \log \sqrt{\rho}\theta}{\partial u}xy\\ &+ 2\left(\frac{\partial \log \sqrt{\rho}\theta}{\partial u}\frac{\partial \log \sqrt{\rho}\theta}{\partial v} - e\right)xz + 2\rho\frac{\partial \log \sqrt{\rho}\theta}{\partial u}xw\\ &- \frac{2}{\theta}\frac{\partial \log \sqrt{\rho}\theta}{\partial v}yz + 2gyw - 2\rho\frac{\partial \log \sqrt{\rho}\theta}{\partial v}zw = 0,\end{aligned}$$

where g is the parameter of the pencil.

* The last part of this theorem is due to Tzitzeica, Comptes Rendus, 30 Nov., 1908.

These quadrics determine an involution on the line MM_1. The equation of the involution is

$$y^2 + 2g\theta^2 yw + \rho^2\theta^2 w^2 = 0.$$

The double points of the involution are given by

$$y + gw\theta^2 = 0, \qquad g = \pm\frac{\rho}{\theta}. \tag{32}$$

Comparing this result with (25), we have

THEOREM 5. *Each pencil of quadrics determined by a pair of the conics* (28) *and* (29) *meets the line* MM_1 *in conjugate pairs of an involution whose double points are the focal points of* MM_1 *in the congruence of these lines.*

For each value of e in general two of the quadrics of the pencil (31) are cones. They correspond to the values of g which make the discriminant of (31) vanish. This discriminant equated to zero is equivalent to

$$ef(\rho^2 - g^2\theta^2) = 0.$$

When $e = 0$, the corresponding conic of the pencil (28) is the line $M^{-1}M'$ counted twice. The corresponding conic (29) meets $M^{-1}M'$ in a single point and consequently all the quadrics (31) are cones whose vertices are on this line. Similar results follow when we take $f = 0$. Excluding these two cases, we get equations (32) again. Hence we have

THEOREM 6. *The cones of a pencil of quadrics* (31) *are tangent to the lines* MM_1 *at its focal points, unless all the quadrics of the pencil are cones.*

The coördinates of the vertex of either cone are given by the corresponding determinants of the third order of the discriminant of (31). These are found to be for

$$\begin{aligned} &g\theta + \rho = 0, \qquad \left[\frac{1}{\theta}\frac{\partial}{\partial v}(\rho\theta^2),\ \frac{\partial \log \sqrt{\rho}\theta}{\partial u}\frac{\partial}{\partial v}(\rho\theta^2) - e\rho\theta^2,\ 0,\ -e\theta\right], \\ &g\theta - \rho = 0, \qquad \left[0,\ \frac{\partial \log \sqrt{\rho}\theta}{\partial v}\frac{\partial}{\partial u}(\rho\theta^2) - e\rho\theta^2,\ \frac{1}{\theta}\frac{\partial}{\partial u}(\rho\theta^2),\ e\theta\right]. \end{aligned} \tag{33}$$

In § 2 we showed that the lines $M^{-1}M_1^{-1}$ and $M'M_1'$ pass through F_1 and F_2 respectively. We shall show that the vertices (33) lie on these respective lines. In fact, it follows readily from (10), (11) and (25) that the coördinates of these points are of the respective forms.

$$\frac{\partial}{\partial v}\rho\theta^2 \cdot x^{-1} - e\theta X_1, \qquad \frac{\partial}{\partial u}\rho\theta^2 \cdot x' - e\theta X_2. \tag{34}$$

We consider now the congruences of lines $M^{-1}M_1^{-1}$ and $M'M_1'$. From Theorem 2 we have that F_1 and F_2 are focal points of these lines in

the congruences. In order to find the other focal points, we differentiate the expressions (34) respectively with respect to v and u. By means of (10), (11), (21), (22) and (25) the resulting expressions are reducible to

$$\left[\frac{\partial^2}{\partial v^2}(\theta\rho^2) - \frac{\partial}{\partial v}(\rho\theta^2)\cdot\frac{\partial}{\partial v}\log\sqrt{\rho}\right]x^{-1} - \frac{\partial}{\partial v}(e\theta)X_1 + \frac{\partial}{\partial v}(\rho\theta^2)(h-e)x,$$

$$\left[\frac{\partial^2}{\partial u^2}(\rho\theta^2) - \frac{\partial}{\partial u}(\rho\theta^2)\frac{\partial}{\partial u}\log\sqrt{\rho}\right]x' - \frac{\partial}{\partial u}(e\theta)X_2 + \frac{\partial}{\partial u}(\rho\theta^2)(k-e)x.$$

From these expressions it follows that when $e = h$, the vertices of the cones are the focal points of these congruences. Hence we have the theorem of Tzitzeica:*

THEOREM 7. *The pencil of quadrics determined by the osculating conics contain two cones whose vertices are focal points of the lines $M^{-1}M_1^{-1}$ and $M'M_1'$.*

It is our purpose now to show that every congruence conjugate to a conjugate system with equal point invariants gives a transformation K of the given conjugate system.

Equation (20) may be written

$$\frac{\partial^2}{\partial u\partial v}(\theta\sqrt{\rho}) = \left(\frac{1}{\sqrt{\rho}}\frac{\partial^2\sqrt{\rho}}{\partial u\partial v} - c\right)\theta\sqrt{\rho},$$

and its adjoint is

$$\frac{\partial^2}{\partial u\partial v}\left(\frac{\mu}{\sqrt{\rho}}\right) = \left(\frac{1}{\sqrt{\rho}}\frac{\partial^2\sqrt{\rho}}{\partial u\partial v} - c\right)\frac{\mu}{\sqrt{\rho}}.$$

Hence the solutions of the given equation and its adjoint may be paired by means of the relation

$$\mu = 2\rho\theta. \tag{35}$$

Suppose then that we have a solution μ. This determines a congruence conjugate to the given system. If we take for θ the value given by (35), we find that the corresponding conjugate system is given by (22), which shows that the congruence is that of a transformation K.

We consider a single application of this result. Let Σ be a surface referred to its lines of curvature and let x, y, z be its rectangular coördinates. Each solution of its point equation leads to a surface S_0 cut by the developables of the normals to Σ in a conjugate system, which necessarily is conjugate to this congruence. If this conjugate system has equal point invariants, it follows from the above result that the points harmonic of the points of S_0 with respect to the centers of principal curvature of Σ

* L. c.

determine a second conjugate system with equal point invariants conjugate to the normal congruence. In this case Σ is a so-called *surface* Ω. Hence the necessary and sufficient condition that Σ be a surface Ω is found by expressing the condition that on an S_0 the conjugate system has equal point invariants.*

PRINCETON UNIVERSITY.

* We have derived the analytical condition for surfaces Ω in the Transactions of the American Mathematical Society, vol. 16, pp. 280–283. This condition is more readily obtained by making use of the results of the present paper.

ON THE DERIVATIVES OF A FUNCTION AT A POINT.*

By J. F. Ritt.

1. It was at the suggestion of Professor Kasner that we undertook to find whether to every sequence of finite numbers $a_1, a_2, \cdots, a_n, \cdots$, where $\sqrt[n]{|a_n|/n!}$ need not remain bounded as n increases indefinitely, there corresponds a function of z whose nth derivative for $z = 0$ is a_n; that is, at least in the real domain.

We have since learned that this question had already been settled in the affirmative by Borel† and by Serge Bernstein.‡ Borel's method involves the solution of an infinite system of linear equations. Bernstein employed his normal series for the purpose. These two methods differ entirely from each other and from the method used in this paper. Borel applied his method to the general theory of infinite systems of linear equations. Bernstein considered the case where the derivatives at several points are assigned in advance. We shall arrive in this paper at results which do not seem to flow from the other two solutions. In particular, we shall settle some questions raised several years ago by Van Vleck.§

2. Consider the series

$$\sum u_n = \sum_{n=1}^{\infty} \frac{a_n z^n}{n!} (1 - e^{-(1/b_n z^2)})^{p_n},$$

where p_n, which may vary with n, is any integer not less than unity and where $p_n < b_n > 2^{p_n - 1}|a_n|$.

Observe that while each a_n may be any complex number, the above inequality requires each b_n to be real and positive.

To obtain a function with the desired derivatives, it would suffice to take $p_n = 1$ for every value of n, and the convergence discussions which follow would become extremely simple. Still we shall discuss the more general case in full, as it will lead to an interesting result.

We shall consider first the behavior of Σu_n in the domain composed of those points $z = x + yi$ for which $y^2 \leqq m^2 x^2$, where $m^2 < 1$. In this

* Read before the American Mathematical Society, Feb. 27, 1915, and Dec. 27, 1915.

† Borel, "Sur quelques points de la théorie des fonctions," Ann. de l'Ec. Norm., 1895, p. 38.

‡ D'Adhémar, "Principes de L'Analyse," vol. II, p. 272. I am indebted to Dr. G. A. Pfeiffer for this reference.

§ Van Vleck, "Divergent series and continued fractions," The Boston Colloquium Lectures, p. 84.

sector, which is limited by the lines $y = mx$ and $y = -mx$, and which contains the axis of real numbers, we have

$$\cos 2\theta \geqq \frac{1 - m^2}{1 + m^2},$$

where θ is the amplitude of z. Incidentally, the real part of $1/z^2$ is positive.

One sees readily that in this sector the Cauchy function $e^{-(1/z^2)}$ approaches zero uniformly with z, and has zero derivatives of all orders at the origin, if it is given there the value zero.

We shall show now that Σu_n is convergent in the domain under consideration, and that all its derived series are uniformly convergent in every portion of that domain in which $|z|$ is bounded, so that, since

$$u_n = \frac{a_n z^n}{n!}\left[1 - p_n e^{-(1/b_n z^2)} + \frac{p_n(p_n - 1)}{2!} e^{-(2/b_n z^2)} - \cdots + (-1)^{p_n} e^{-(p_n/b_n z^2)}\right],$$

Σu_n has the desired derivatives for $z = 0$.*

We use, for this purpose, the inequalities

$$|1 - e^{-(1/B)}| < 2$$

when the real part of B is positive, or when $|B| > 1$, and

$$|A(1 - e^{-(1/B)})| < 2$$

when the real part of B is positive and $|B| > |A|$, or when $1 < |B| > |A|$.

The first of these is obvious when the real part of B is positive, for then $|e^{-(1/B)}| < 1$. Hence the second is true when the real part of B is positive and when $|A| < 1$. When $|B| > 1$,

$$(1 - e^{-(1/B)}) = \left|\frac{1}{B} - \frac{1}{2!B^2} + \cdots\right| < \frac{e - 1}{B} < \frac{2}{B},$$

and this fact accounts for the remaining cases.

Now

$$|u_n| = \left|\frac{z^{n-2}}{n!} 2^{p_n - 1} a_n z^2 (1 - e^{-(1/b_n z^2)}) \frac{(1 - e^{-(1/b_n z^2)})^{p_n - 1}}{2^{p_n - 1}}\right|,$$

and since the real part of $b_n z^2$ is positive and $b_n z^2 > 2^{p_n - 1} a_n z^2$, we have by the inequalities above,

$$|u_n| < 2\left|\frac{z^{n-2}}{n!}\right|,$$

from which it is evident that Σu_n is uniformly convergent in any bounded portion of our domain.

* The sufficiency of these conditions is generally proved only for real functions of a real variable. It is not difficult to show that they suffice also in the present case.

Take now the first derived series

$$\Sigma u_n' = \sum_{n=1}^{\infty}\left[\frac{a_n z^{n-1}}{(n-1)!}(1-e^{-(1/b_n z^2)})^{p_n} - \frac{2p_n a_n z^{n-3}}{b_n n!}(1-e^{-(1/b_n z^2)})^{p_n-1}e^{-(1/b_n z^2)}\right].$$

Consider the four series

$$\Sigma\alpha_n = \sum_{n=1}^{\infty}\frac{a_n z^{n-1}}{(n-1)!}(1-e^{-(1/b_n z^2)})^{p_n}, \qquad \Sigma\beta_n = \sum_{n=1}^{\infty}\frac{p_n a_n}{b_n}\frac{z^{n-3}}{n!}(1-e^{-(1/b_n z^2)})^{p_n},$$

$$\Sigma\gamma_n = \sum_{n=1}^{\infty}\frac{r_n a_n}{b_n}\frac{z^{n-3}}{n!}(1-e^{-(1/b_n z^2)})^{p_n-1}, \qquad \Sigma\delta_n = \sum_{n=1}^{\infty}\frac{s_n a_n}{b_n}\frac{z^{n-3}}{n!},$$

where $r_n = p_n$ or 0 according as $p_n > 1$ or $p_n = 1$, and $s_n = 0$ or 1 according as $p_n > 1$ or $p_n = 1$.

The series $\Sigma\alpha_n$, $\Sigma\beta_n$ and $\Sigma\gamma_n$ do not differ materially in form from Σu_n. This is quite evident in the case of $\Sigma\alpha_n$. It becomes apparent also for $\Sigma\beta_n$ and $\Sigma\gamma_n$ if we ignore the first three terms of those series, and consider that, since $b_n > p_n$, $|p_n a_n / n(n-1)(n-2)b_n| < |a_n| < b_n 2^{p_n-1}$. Hence any property of Σu_n which arises from the fact that $p_n < b_n > 2^{p_n-1}|a_n|$ is enjoyed also by $\Sigma\alpha_n$, $\Sigma\beta_n$ and $\Sigma\gamma_n$. The series $\Sigma\delta_n$, if we drop its first two terms, becomes an entire function.

Hence, we may write

$$\Sigma u_n' = \Sigma\alpha_n + 2\Sigma\beta_n - 2\Sigma\gamma_n - 2\Sigma\delta_n,$$

so that $\Sigma u_n'$ converges uniformly wherever Σu_n does, and represents the derivative of Σu_n. The series $\Sigma\delta_n$ can be differentiated formally any number of times, and the series $\Sigma\alpha_n$, $\Sigma\beta_n$ and $\Sigma\gamma_n$, like Σu_n, at least once. Hence the second derivative of Σu_n exists and can be obtained formally. Thus, if Σu_n can be differentiated formally n times, the next formal differentiation will also be valid. As remarked above, it is evident that the nth derivative, for $z = 0$, is a_n.* It should be emphasized that when we speak of derivatives at the origin, we understand that z is confined to the sector described above.†

Similarly, the function

$$\sum_{n=1}^{\infty}\frac{a_n z^n}{n!}(1-e^{-(1/b_n y)}),$$

where $1 < b_n > |a_n|$ and $y = z$ or $-z$, according as the real part of z is

* Evidently the problem of finding the most general function with the desired derivatives is identical with that of finding the most general function with zero derivatives.

† In general the sides of the sector cannot be rotated beyond the lines $y = x$ and $y = -x$, without destroying the regularity of the behavior of Σu_n. For, if the derivatives should happen to exist relative to a sector of opening greater than $\pi/2$, a slight change of one of the b's would destroy the regularity outside of the lines $y = x$ and $y = -x$. Cf. Van Vleck, loc. cit.

positive or is negative, will have the desired derivatives for $z = 0$. Here our domain is the entire z-plane, excepting those points for which $cos^2 \theta < \epsilon$, θ being the amplitude of z and ϵ an arbitrarily small positive number. Thus while, when lim. sup. $\sqrt[n]{|a_n|/n!} = \infty$, there exists no function which has the desired derivatives relative to a domain of which the origin is an interior point, the above example permits us to come as close as we desire to a complete envelopment of the origin. By using the function $e^{-(1/\sqrt{r})}$ one could hope to cover one of the two narrow gaps still left in our domain, but we shall not go into the convergence investigations.

3. We wish to show that the function Σu_n of § 1 can be developed in a Laurent series, convergent everywhere except at the origin. For this purpose we shall show that Σu_n is uniformly convergent within the ring formed by two circles, with centers at the origin, and with any radii $r > 0$ and $R > r$ respectively.

If $b_n r^2 \leqq 1$, we have when $|z| > r$, since $|a_n| < b_n > p_n$,

$$|u_n| < \frac{(1 + e^{1/r^2})^{1/r^2}}{r^2} \left| \frac{z^n}{n!} \right|.$$

If $b_n r^2 > 1$, we have, by the inequalities of § 1,

$$|u_n| < 2 \left| \frac{z^{n-2}}{n!} \right| < \frac{2}{r^2} \left| \frac{z^n}{n!} \right|.$$

From the above upper limits for $|u_n|$ the uniform convergence of Σu_n within the ring in question is apparent. Hence Σu_n admits of development in a Laurent series, convergent everywhere except at the origin, which can be gotten by adding up the developments of the terms u_n. Let

$$\sum u_n = \sum_{n=0}^{\infty} \alpha_n z^n + \sum_{n=1}^{\infty} \beta_n z^{-n}.$$

If lim. sup. $\sqrt[n]{|a_n|/n!} = \infty$, the principal parts of the derivatives are evidently contributed by the negative power series $\Sigma \beta_n z^{-n}$. One naturally inquires as to whether one can find a series of *negative powers alone* which has any desired derivatives at the origin. Such a series we shall in fact obtain by taking each p_n sufficiently large, since the exponent of the highest power of z, in u_n, is $n - 2p_n$.

Having obtained such a series of negative powers, we can, by adding terms of the form $Kz^{-n}e^{-1/z^2}$, reduce any finite number of coefficients to any values desired, without affecting the derivatives at the origin. Thus, being given any sequence of numbers, $a_1, a_2, \cdots, a_n, \cdots$, and any function $\sum_{n=1}^{n=m} \beta_n z^{-n}$, we can, in an infinite number of ways, determine a series $\sum_{n=m+1}^{\infty} \beta_n z^{-n}$,

such that $\sum_{n=1}^{\infty} \beta_n z^{-n}$ has a_n as its nth derivative at $z = 0$, provided z remains in the domain described in connection with the function e^{-1/z^2}.

The delicate adjustment of coefficients which, when z remains in a limited domain, gives the series $\Sigma\beta_n z^{-n}$ a finite value and definite derivatives of all orders for $z = 0$, at which point each term $\beta_n z^{-n}$ becomes infinite, suggests interesting investigations. However, all our attempts to discover the nature of this adjustment have thus far been without significant result.

4. We shall extend the results of § 1 to the case of n variables, each variable remaining in a sector similar to that described in connection with the function e^{-1/z^2}. That is, assuming all differentiations commutative, we shall show the existence of a function with any desired partial derivatives for $x_1 = x_2 = \cdots = x_n = 0$. For simplicity of notation we limit ourselves to two variables, but the generality of the principle employed will be apparent.

Consider the series

$$\sum u = \sum \frac{a_{p,q} x_1^p x_2^q}{p!q!} (1 - e^{-\frac{1}{b_{p,q} x_i^2}}),$$

where i is to be either 1 or 2, and where $1 < b_{p,q} > N \mid a_{p,q} \mid$, N being the number of terms in a homogeneous polynomial of degree $p + q$. The significance of $a_{p,q}$ is evident. We wish to choose i in each term in such a way that there may be only a finite number of terms in which a factor $1 - e^{-1/b_{p,q} x_1^2}$ occurs, and in which the exponent of x_1 is less than any positive integer M; similarly for x_2. The purpose of this is that only a finite number of negative powers may be introduced at each differentiation. It will suffice, for instance, to take $i = 1$ if $p \geqq q$ and $i = 2$ if $p < q$.

Writing

$$\sum \mid u_n \mid = \sum_{n=1}^{\infty} \sum_{p=0}^{p=n} \frac{\mid a_{n-p,\,p} x_1^{n-p} x_2^p (1 - e^{-\frac{1}{b_{n-p,\,p} x_i^2}}) \mid}{(n-p)!p!},$$

one recognizes readily that Σu_n is absolutely and uniformly convergent, within any finite limits, provided x_1 and x_2 remain in the domains described above. The remainder of the discussion will be similar to that in the case of one variable if one separates Σu into two series, the first formed of those terms which contain $1 - e^{-1/b_{p,q} x_1^2}$ as a factor, the second formed of the remaining terms. Corresponding to the power series $\Sigma\delta_n$ there will appear two power series in two variables whose majorants are everywhere convergent. All derivatives will be continuous with respect to both variables. Hence, as far as the real domain is concerned, the dif-

ferentiations will be commutative.* But since the derivatives in the real domain determine the derivatives in the entire domain under consideration, the differentiations in the entire domain are commutative.

COLUMBIA UNIVERSITY.

* Of course, if the derivatives are complex, we must consider the real parts and imaginary parts separately.

AN EXISTENCE THEOREM FOR THE SOLUTION OF A TYPE OF REAL MIXED DIFFERENCE EQUATION.

By Albert A. Bennett.

1. A Mixed Difference Equation. An equation of the form

$$y_{h+1}^{(0)} = F[x; y_0^{(0)}, y_0^{(1)}, \cdots, y_0^{(k)}; y_1^{(0)}, y_1^{(1)}, \cdots, y_1^{(k_1)}; \cdots; y_h^{(0)}, y_h^{(1)}, \cdots, y_h^{(k_h)}], \tag{1}$$

where $y_i^{(j)}$ denotes $(d^j/dx^j)y(x+i)$, is called a mixed difference equation, although not of the most general type. The numbers, h, k, k_1, k_2, $\cdots$, k_h, are, of course, non-negative integers, and either k or one of the numbers k_i, $i = 1, 2, \cdots, h$ must be positive, in order that the equation may not reduce to an ordinary difference equation. We shall confine ourselves to the particularly interesting case in which the integer k is greater than any one of the integers k_i, $i = 1, 2, \cdots, h$, no other restriction being imposed upon these numbers. We shall consider F as any function subject to the following restrictions:

(i) $F[x; u_{00}, u_{01}, \cdots, u_{0k}; u_{10}, u_{11}, \cdots, u_{1k_1}; \cdots; u_{h0}, u_{h1}, \cdots u_{hk_h}]$ is real and finite in the composite real domain of the arguments defined as independent variables for which x is real, finite and non-negative, and each u_{ij} is real and finite but either positive or negative.

(ii) Every partial derivative of F of any order and with respect to any of the arguments, exists in the domain above mentioned.

(iii) $\partial F/\partial u_{0k}$ does not vanish in the domain.

It should be noted that while F is finite, it need not be bounded in the domain.

We shall examine the nature of the solutions of equation (1) for x real and non-negative.

2. The Continuity of Every Solution and of Its Derivatives. In the theory of ordinary and of mixed difference equations it is frequently convenient to consider functions $f(x)$ which present singularities for certain isolated values of x. Thus at a point a, $f(x)$ may be undefined, while in a sufficiently small neighborhood on the right $f(x)$ may be defined and continuous, and similarly on the left. If the limit of $f(x)$ exists as x approaches the value a from the right, this limit may be denoted by $f(a+)$. The expression $f(a-)$ may be defined analogously. We may generalize the equation (1) slightly by regarding $y_i^{(j)}$ as denoting $(d^j/dx^i)y(x+i)$

for points at which $y_i^{(j)}$ and its jth derivative exist and are continuous, while permitting also the existence of certain isolated points a for which $y_i^{(j)}$ denotes the limit of $(d^j/dx^i)y(x+i)$ as x approaches a from the right or again as x approaches a from the left. In the usual theory of real difference equations, discontinuous solutions may be constructed with the greatest ease, while solutions continuous at all points on the positive real axis are obtained only when additional boundary conditions are introduced, and fresh boundary conditions must be satisfied for every additional derivative that is required to be continuous. Furthermore by a suitable definition at the points of discontinuity, discontinuous solutions and solutions with discontinuous derivatives of suitable order may be obtained in the usual theory.

That discontinuous functions or functions with no derivatives of order higher than a given number at certain points, may exist which satisfy equation (1) is more or less obvious, provided that the symbols $y_i^{(j)}$ be interpreted in the more general sense above mentioned. We shall however in the following regard y_i^j as originally defined. The existence of a solution is no longer obvious, particularly in view of a theorem that we shall now prove.

For equation (1) to have a meaning, $y(x)$ must exist together with its first k derivatives for any positive values of x, while for the end point $x=0$, the derivatives are regarded as existing on the right only. In particular for any non-negative point x_0, $y^{(k)}(x_0)$, $y^{(k)}(x_0+1)$, $\cdots$, $y^{(k)}(x_0+h)$, and also $y'(x_0+h+1)$ must be supposed to exist. Now (1) when regarded as an implicit equation defining $y^{(k)}(x_0)$, in terms of the other quantities, may be solved for $y^{(k)}(x_0)$, since by hypothesis $\partial F/\partial[y^{(k)}(x_0)]$ does not vanish in the domain. The resulting equation may be differentiated totally with respect to x, and evaluated for $x=x_0$. The form of this last equation in terms of the partial derivatives of F is readily obtained as follows: Let us define G by the identical relation,

$$y_0^{(k)} \equiv G[x; y_0^{(0)}, y_0^{(1)}, \cdots, y_0^{(k-1)}; y_1^{(0)}, \cdots, y_1^{(k_1)}; \cdots; y_h^{(0)}, \cdots, y_h^{(k_h)}; F].$$

Differentiating equation (1), we have

$$\begin{aligned} y_{h+1}^{(1)} = {} & F_x[x; y_0^{(0)}, y_0^{(1)}, \cdots, y_0^{(k-1)}, G; y_1^{(0)}, \cdots, y_1^{(k_1)}; \cdots; y_h^{(0)}, \cdots, y_h^{(k_h)}] \\ & + F_{y_0^{(0)}} \cdot y_0^{(1)} + F_{y_0^{(1)}} \cdot y_0^{(2)} + \cdots + F_{y_0^{(k-1)}} \cdot G + F_G \cdot G' \\ & + F_{y_1^{(0)}} \cdot y_1^{(1)} + \cdots + F_{y_1^{(k_1)}} \cdot y_1^{(k_1+1)} + \cdots + F_{y_h^{(0)}} \cdot y_h^{(1)} \\ & + \cdots + F_{y_h^{(k_h)}} \cdot y_h^{(k_h+1)}. \end{aligned}$$

where $F_G \equiv F_{y_0^{(k)}} \neq 0$. Solving for G', we obtain the equation desired in the form

$$y_0^{(k+1)} = G' = \frac{1}{F_{y_0^{(k)}}}[y_{h+1}^{(1)} - F_x + F_{y_0^{(0)}} y_0^{(1)} - \cdots - F_{y_0^{(k-1)}} \cdot y_0^{(k)} - \cdots - F_{y_h^{(k_h)}} y_h^{(k_h+1)}]$$

where $y_0^{(k)}$ is throughout replaced by its value in terms of the other quantities. The terms of the right hand member are all determinate throughout the entire domain considered, so that $y_0^{(k+1)} = y^{(k+1)}(x_0)$ must be regarded as existent at every non-negative x_0. It is here that we make use of the fact that k is greater than any one of the integers k_i, $i = 1, 2, \cdots, h$. By replacing x_0 by $x_0 + i$ we conclude the existence of $y_i^{(k+1)}$, $i = 1, 2, \cdots, h$. The entire reasoning may then be repeated to show the existence of $y_0^{(k+2)}$, etc. By successive applications we prove the existence of each element in the following doubly infinite array as a consequence of the supposed existence of a solution, the array being $y_i^{(k+l)}$, $l = 0, 1, 2, \cdots$, $i = 0, 1, 2, \cdots$.

We shall speak of values assumed by the following expressions, as the *initial values* of $y(x)$, viz., $y(x_0)$, $y'(x_0)$, $\cdots$, $y^{(k)}(x_0)$; $y(x_0 + 1)$, $y'(x_0 + 1)$, $\cdots$, $y^{(k_1)}(x_0 + 1)$; $\cdots$; $y(x_0 + h)$, $y'(x_0 + h)$, $\cdots$, $y^{(k_h)}(x_0 + h)$, where x_0 takes on all values for which $0 \leq x_0 < 1$. The initial values are therefore infinite rather than finite in number. We now have the theorem:

THEOREM. *Every solution of* (1), *having real and finite initial values, is continuous with all of its derivatives at all finite points on the positive real x-axis.*

3. Power Series Representing a Solution. It will be granted that there exist equations of the form (1) having solutions. We shall for the moment consider the nature of a power series representing a solution supposed to exist without entering into the question as to when such a solution exists. When once the form of the solution is known, we will be prepared to prove that a solution always exists.

Let us consider a given function $y(x)$, which is continuous with all of its derivatives on the positive real axis. At any point of the positive real axis, the function $y(x)$ may be expanded as a Taylor's series in finite form, where the degree of the highest term in $(x - x_1)$ is arbitrarily preassigned. We are led to an infinite Taylor's series at the point x_1, which will however in general be divergent for every value of x different from x_1. The function completely determines the series, and the series completely determines the value of the function and of all of its derivatives at the point x_1. We may therefore regard the series, even when divergent as representing the function at the point x_1, although perhaps not representing the function at any other point. The series while determining the differential coef-

ficients may not determine a function element. If $S(x)$ denote the series, we may write

$$y(x) \sim S(x) \equiv a_0 + a_1(x - x_1) + \cdots + a_n(x - x_1)^n + \cdots.$$

As is usual* in the theory of divergent power series if $y_1(x) \sim S_1(x)$, and $y_2(x) \sim S_2(x)$, then $(y_1 + y_2) \sim (S_1 + S_2)$, $(y_1 \times y_2) \sim (S_1 \times S_2)$ and if (y_1/y_2) is finite $(y_1/y_2) \sim (S_1/S_2)$ also $y_1^n \sim S_1^n$, where the operations are performed formally, as with convergent power series. In the usual theory, the series S is regarded as initially given, and the function y as determined from S. It then occurs that in general we cannot say that $y' \sim S'$ where y' is the derivative of $y(x)$ at $x = x_1$, and S' is obtained by differentiating S term by term. When we use the fact that, as in the present case, $y(x)$ is given, and is continuous together with all of its derivatives in the neighborhood of $x = x_1$, we see from the nature of Taylor's series, that $y^{(m)} \sim S^{(m)}$, for every positive integer m. Hence we conclude that *if equation* (1) *has a solution* $y(x)$ *with real finite initial values,* $y(x)$, *can be represented at every point* $x_1 \geq 0$, *by a series* S, *in powers of* $x - x_1$, *which is such that* $y \sim S(x)$, *and* $y^{(m)} \sim S^{(m)}(x)$, *where* m *is any positive integer.*

The power series which represents a solution y, at one of the points $x_1 = x_0$, $x_0 + 1$, $\cdots$, $x_0 + h$, will be spoken of as an *initial series* of y, for x_0. For the given point x_1, and the given solution y, the initial series is, of course, unique. For a given x_0, there will be for y, $h + 1$ initial series corresponding to $x_1 = x_0$, $x_0 + 1$, $\cdots$, $x_0 + h$. From the nature of the equation (1), the series representing a solution $y(x)$, at a point $x_1 = x_0 + d$ where d is a positive integer greater than h, will be determined completely by the $h + 1$ initial series of y for x_0, and the only restrictions upon the behavior of y between x_0 and $x_0 + 1$, are the end conditions requiring y and its derivatives, to approach the given values at x_0, and x_1, and the general conditions that the function and its derivatives be continuous.

4. The Existence of Solutions with Assigned Initial Series. The situation arising with regard to the number of arbitrary conditions that may be imposed upon a solution of the equation (1) is in marked distinction to that occurring, for example, in the usual theory of linear differential equations. In the first place the initial series for x_1 and x_2 where $0 \leq x_1 < x_2 < 1$, are entirely independent of each other, a fact which we have already mentioned. This is a feature common to all difference equations. The noteworthy fact concerning the equation (1) may be stated as follows:

* Cf. Borel, Leçons sur les séries divergentes, Borel Series, and Van Vleck, Selected Topics, etc., Boston Colloquium.

THEOREM. *Any $h + 1$ series, divergent if desired, may be chosen arbitrarily as the initial series for $x = 0$, of a solution of equation* (1). *There will then exist an infinite number of distinct functions, $y(x)$, all of which satisfy* (1), *which have the given series as initial series and which are continuous with all of their derivatives for all positive real values of x. For each positive integral value d of x, there will be a series uniquely determined by the initial series and the point d which is the common Taylor's series for all of these solutions, $y(x)$.*

The above theorem will be demonstrated, if we can construct a function $f(x)$ defined for x in the interval $0 \leq x < h + 1$, with the assigned initial series at the points $x = i$, $i = 0, 1, \cdots, h$, and with a series representation at $x = h + 1$, identical with that determined by (1) from the assigned initial series, the function $f(x)$ being continuous together with all of its derivatives within and at the extremities of the interval. For the equation (1) will then determine the value of $y(x)$ and of its derivatives at $x = h + 1$, and these will coincide with the values already determined for this point, if $y(x)$ be defined as equal to $f(x)$ for $0 \leq x < h$. The equation (1) will then define $y(x)$ over the entire positive real axis. The function $f(x)$ is further supposed to contain at least one arbitrary constant. We shall prove the existence of such a function by exhibiting a function $f(x)$ which satisfies not only these but also more stringent conditions.

5. The Existence of a Function with Assigned Series at an Infinite Number of Points. We shall now prove the following theorem:

THEOREM. *If any point x_0 on the real x-axis be selected, there exists a real function $f(x)$, containing an infinite number of arbitrary real parameters, but which regarded as a function of x is continuous together with all of its derivatives at every finite real point of the x-axis for every choice of the parameters. Also the Taylor's series of $f(x)$ at each of the infinite array of points, $x = x_0 + i$, $i = , \cdots, -2, -1, 0, 1, 2, \cdots$, is independent of the values of the parameters, being previously assigned for each of these points independently, without regard to convergence or the behavior at other points.*

To demonstrate the truth of this theorem, we shall first exhibit a function $f_i(x)$ which is finite and continuous for all real finite values of x, which vanishes with all of its derivatives at the points $x = x_0 + i + j$, $j = \cdots, -2, -1, 1, 2, 3, \cdots$, and which has at the point $x = x_0 + i$, the preassigned Taylor's series associated with this point, viz.,

$$a_{i,0} + a_{i,1}(x - x_0 - i) + a_{i,2}(x - x_0 - i)^2 + \cdots + a_{i,n}(x - x_0 - i)^n + \cdots.$$

The function $f_i(x)$ will itself be obtained in the form $f_i(x) \equiv \sum_{n=0}^{\infty} u_{i,n}$,

where

$$u_{i,n} \sim 0 + \cdots + 0 + a_{i,n}(x - x_0 - i)^n + 0 + \cdots.$$

The final function $f(x)$ will be defined as $\sum_{i=-\infty}^{\infty} f_i(x)$. Each of the functions $u_{i,n}$ will involve in its definition an arbitrary real positive parameter $b_{i,n}$.

6. The Definition of $u_{i,n}$. The function $u_{i,n}$ may be defined in numerous different manners. Perhaps the simplest definition is suggested by the function constructed by Mr. J. F. Ritt.* He has noted that the function

$$v_n = \frac{a_n z^n}{n!}(1 - e^{-(1/b_n z^2)})^{p_n},$$

where $p_n < b_n > 2^{p_n - 1}|a_n|$, and where p_n is always an integer not less than one, is such that $\sum_{n=1}^{\infty} v_n$ converges uniformly, and absolutely together with all of its derivatives at every point $z = x + iy$ for which $y^2 \leq m^2 x^2$, where $m^2 < 1$. On the other hand the function represented in the region considered will have at the origin the number a_n as the nth differential coefficient, for methods of approach which lie in the region. The series of numbers a_n may be assigned as arbitrary complex quantities without regard to convergence.

When we form the product

$$\frac{1}{1 + e^{\frac{1}{4z^2 - 1}\frac{1}{z^2(1-z^2)}}} \Sigma v_n = g(z),$$

we obtain a function having the same differential coefficients at the origin when approached in the above region, and whose corresponding coefficients at $z = 1$, when approached from the left and $z = -1$, when approached from the right are all zero. For, indeed, the factor $1/(1 + e^{(4z^2-1)/z^2(z^2-1)})$ is finite in the region considered, while its expansions at the origin, the point $z = 1$, and the point $z = -1$ are respectively those of $(1 - e^{-(1/z^2)})$, $(e^{-(1/1-z)})$, and $(e^{-(1/1+z)})$ owing to the peculiarity of the function $e^{-(1/z^2)}$ at the origin. We are concerned only with the real axis in the present discussion. We may now define $u_{i,n}$ as follows:

$$u_{i,n} = \frac{a_{i,n}\{1 - e^{-\frac{1}{b_{i,n}[x-(x_0+i)]^2}}\}^{p_{i,n}}}{1 + e^{\frac{1}{4[x-(x_0+i)]^2-1}\frac{1}{[x-(x_0+i)]^2\{1-[x-(x_0+i)]^2\}}}} x^n, \qquad \text{for} \qquad |x - (x_0 + i)| \leq 1,$$

* *Annals of Mathematics*, vol. 18, pp. 18–23.

$u_{i,n} \equiv 0$ for $|x - (x_0 + i)| \geq 1$, $-\infty < i < \infty$, $0 \leq n < \infty$, where $b_{i,n}$ is any real positive constant such that, $b_{i,n} > 2^{p_{i,n}-1}|n!\, a_{i,n}|$, and $p_{i,n}$ is any integer, > 0, $< b_{i,n}$.

With this definition, $f_i(x) = \sum_{n=0}^{\infty} u_{i,n}$ is a real function of x, continuous with all of its derivatives along the entire real axis and vanishing with all of its derivatives for $|x - (x_0 + i)| \geq 1$, while the Taylor's series for $f_i(x)$ at $x = x_0 + i$ is simply $\sum_{n=0}^{\infty} a_{i,n}[x - (x_0 + i)]^n$.

The series $\sum_{i=-\infty}^{+\infty} f_i(x)$ will then be absolutely and uniformly convergent for all real values of x, with an ascribed Taylor's series at each point $x_0 + i$, $-\infty < i < +\infty$ i, *an integer*. Also the function $f(x)$, represented by $\sum_{i=-\infty}^{+\infty} f_i(x)$, is continuous together with all of its derivatives at every real finite point, which establishes the theorem.

7. Some References to the Recent Literature. The following references to the most recent literature concerning questions related to those here discussed may prove of interest.

Mixed Difference Equations.

O. Polusuchin, Diss., Zürich, 1900.

E. Schmidt, Math. Ann., 70 (1911), p. 499 ff.

F. Schürer, Ver. d. K. Sächs, Ges. d. Wiss., 64 (1912), p. 167–236, and 66 (1914), p. 137–159.

H. Bateman, Proc. Fifth Int. Cong. Math. (1912), p. 291–294.

Functions with Assigned Taylor's Series

E. Borel, Leçons sur les Fonctions de Var. Reélles, Borel Ser., 1905.

S. Bernstein, Note in d'Adhemard's Leçons de l'Analyse, II, p. 239–283.

J. F. Ritt, *Annals of Math., loc. cit.*

PRINCETON UNIVERSITY,
November, 1915.

DOUBLE ELLIPTIC GEOMETRY IN TERMS OF POINT AND ORDER ALONE.*

By J. R. Kline.

1. Introduction.

In his Rational Geometry,† Halsted built up two-dimensional double elliptic geometry, in terms of the undefined symbols point, order, association and congruence. In the present paper I propose a categorical set of ten mutually independent axioms for three-dimensional double elliptic geometry. Only the symbols point and order are undefined.

I wish to express my deep gratitude to Professor Robert L. Moore, who suggested the problem of this paper and aided me continually in its preparation.

2. Axioms and Definitions.

Axiom I. If A is a point, then there exists at least one point A', different from A, such that $AA'C$‡ is false for every C.

Definition 1. If A and B are distinct points such that ABC is false for every C, then B is said to be an *opposite* of A. If A is a point, A' denotes an opposite of A.

Axiom II. There exist two distinct points A and B such that B is not an opposite of A.

Axiom III. If ABC, then CBA.

Axiom IV. If ABC and A' is an opposite of A, then $A'CB$.

Axiom V. If ABC and ACD, then ABD.

Definition 2. The *line* $AB(A \neq B \neq A')$ is the set of all points $[X]$ such that $X = A$, $X = A'$, $X = B$, $X = B'$, XAB, AXB, ABX or $AX'B$. The set of all points $[X]$ such that AXB constitute the *segment* AB. A and B are the *end points* of this segment.

Axiom VI. If there exist three distinct points, no two of which are opposites, then there exist three distinct points A, B and C such that A is not an opposite of B and such that C is not on the line AB.

Axiom VII. If D is not on the line AB and C and E are such that ABC and BED and if there exists F such that DFA, then there exists G such that CEG and DGA.

* Presented to the Society, April 24, 1915.

† G. B. Halsted, Rational Geometry, John Wiley and Sons, pp. 212–247.

‡ The abbreviation "$AA'C$" signifies that the points A, A' and C are in the order $AA'C$.

DEFINITION 3.* Three non-collinear points A, B, C are the *vertices* of a *triangle* ABC, whose *sides* are the segments AB, BC, CA and whose *boundaries* are its vertices and its sides.

DEFINITION 4. The *interior* of a triangle ABC is the set of all points $[X]$ such that X lies on a segment whose end points are on different sides of the triangle ABC.

DEFINITION 5. If A, B and C are non-collinear points, the *plane* ABC consists of all points collinear with two points of the sides of the triangle ABC.

AXIOM VIII. If there exist three distinct non-collinear points, then there exists a plane ABC and a point D such that D is not on the plane ABC.

DEFINITION 6. If A, B, C and D are four non-collinear points, they are the *vertices* of a *tetrahedron* $ABCD$, whose *faces* are the interiors of the triangles ABC, BCD, CDA, DAB, whose *edges* are the segments AB, BC, CD, DA, AC and BD.

DEFINITION 7. If A, B, C and D are the vertices of a tetrahedron, the *space* $ABCD$ consists of all points collinear with two points of the faces of the tetrahedron $ABCD$.

AXIOM IX. If there exist four distinct points, neither lying on the same line, nor lying in the same plane, then there exists a space $ABCD$ such that there is no point not collinear with two points of the space $ABCD$.

AXIOM X. If all the points of a segment are divided into two mutually exclusive classes $[S_1]$ and $[S_2]$ such that no point of S_1 lies between two points of S_2 and such that no point of S_2 lies between two points of S_1, then there exists H such that if, A is a point of $S_1 \neq H$ and B is a point of $S_2 \neq H$, then AHB.

3. Consequences of Axioms I–V.

THEOREM 1. If A and B are two distinct points and B is not an opposite of A, then there exists C such that ABC.

THEOREM 2. If A_1 is an opposite of A, then A is an opposite of A_1.

Proof. Suppose A is not an opposite of A_1. Then, by Theorem 1, there exists C such that A_1AC. By Axioms III, I, IV and III, A_1AC implies AA_1C'. But AA_1C' is contrary to hypothesis. Hence A is an opposite of A_1.

THEOREM 3. If ABC, then C is different from A, B, every opposite of A and every opposite of B.

* Definitions 3, 4, 5, 6 and 7 and Axioms VIII and IX are the same as Definitions 2, 5, 6, 7 and 8 and Axioms IX and X of Veblen's System of Axioms for Geometry, Transactions of the American Mathematical Society, vol. 5 (1904), page 345.

Case I.—Suppose $C = A$. Then ABA. By Axioms IV, III, IV and III, ABA implies $AA'B'$. But $AA'B'$ is contrary to the Definition of A'. Hence $C \neq A$*.

Case II. Suppose $C = A'$. Then ABA'. By Axiom IV, ABA' implies $A'A'B$. By Axiom III, ABA' implies $A'BA$. By Axiom V, $A'A'B$ and $A'BA$ imply $A'A'A$. By Axiom III, $A'A'A$ implies $AA'A'$, which is contrary to the definition of A'. Hence $C \neq A'$.

Case III. Suppose $C = B$. Then ABB. By Axioms III, IV and III, ABB implies BAB'. But BAB' is contrary to Case II. Hence $C \neq B$.

Case IV. Suppose $C = B'$. Then ABB'. By Axioms IV and III, ABB' implies $BB'A'$, which is contrary to the Definition of B'. Hence $C \neq B'$.

THEOREM 4. If ABC, then not BCA.†

Proof. Suppose ABC and BCA. By Axiom III, BCA implies ACB. By Axiom V, ABC and ACB imply ABB. But ABB is contrary to Theorem 3. Hence not BCA.

THEOREM 5. If two distinct points are opposites of the same point, then they are opposites of each other.

Proof. Suppose the two distinct points A_1 and A_2 are both opposites of A. Then by Theorem 2, A is an opposite of A_1 and of A_2. Suppose A_2 is not an opposite of A_1. Then, by Theorem 1, there exists C such that A_1A_2C. By Axioms IV, III, IV and III, $A_1A_2\ C$ implies CAA. But CAA is contrary to Theorem 3. Hence A_2 is an opposite of A_1. In like manner A_1 is an opposite of A_2.

THEOREM 6. If X is any point, then there exists a point Y different from X and not an opposite of X.

Proof. Suppose there is no such point Y. Then every point either coincides with X or is an opposite of X. By Axiom II, there exist two distinct points A and B such that B is not an opposite of A.

Of the following four conceivable cases, the first two are evidently impossible.

Case I. A is X and B is X.

Case II. A is X and B is an opposite of X.

Case III. B is X and A is an opposite of X, consequently of B. Then, by Theorem 2, B is an opposite of A, which is contrary to hypothesis.

Case IV. A and B are both opposites of X. Then, by Theorem 5, B is an opposite of A, which is contrary to hypothesis.

THEOREM 7. No point has more than one opposite.

Proof. Suppose the point C has two opposites C_1 and C_2. By Theorem 6, there exists a point B, different from C and not an opposite of C. By

* Cf. Axiom IV of Veblen's System, loc. cit., p. 345.

† Cf. Axiom III of Veblen's System, loc. cit., p. 344.

Theorem 1, there exists D such that CBD. By Axiom IV, CBD implies C_1DB and C_2DB. By Theorem 5 and Axiom IV, C_1DB implies C_2BD. By Axiom III, C_2BD implies DBC_2. But by Theorem 4, C_2DB implies not DBC_2. Hence the supposition that C has two opposites leads to a contradiction.

THEOREM 8. If ABC, then $B \neq A$.

Proof. Suppose $B = A$. Then AAC. By Axiom III, AAC implies CAA, which is contrary to Theorem 3.

THEOREM 9. If ABC, then not CAB.

Proof. By Axiom III, ABC implies CBA. By Theorem 4, CBA implies not BAC and hence, by Axiom III, not CAB.

THEOREM 10. Between any two distinct, non-opposite points, there is always a third point.

Proof. Let A and B be any two points such that $A \neq B \neq A'$. By Axiom I and Theorem 7, A has one and only one opposite. If B were the opposite of A', then, by Theorems 2 and 7, B would be the same point as A, contrary to hypothesis. Hence, by Theorem 1, there exists C such that $A'BC$. By Axiom IV and Theorem 2, $A'BC$ implies ACB.

THEOREM 11. If ABC, then not $AB'C$.

Proof. By Axioms III, IV, III, IV and III, $AB'C$ implies $AC'B$. By Axiom V, $AC'B$ and ABC imply $AC'C$. By Axiom III, $AC'C$ implies $CC'A$, which is contrary to the Definition of C'.

THEOREM 12. If ABC and ACD, then BCD.

Proof. By Axiom III, ABC implies CBA. By Axioms III, IV and III, ACD implies CAD'. By Axiom V, CBA and CAD' imply CBD'. By Axioms III, IV and III, CBD' implies BCD.

THEOREM 13. There exist infinitely many points.

Proof. By Axiom II, there exist two points A and B such that B is distinct from A and is not an opposite of A. By Theorem 1, there exists C_1 such that ABC_1. By Theorem 3, C_1 is different from A, A', B, and B'. There exists, by Theorems 1 and 3, a point C_2, different from A, A', C_1 and C_1', such that AC_1C_2. As $C_2 \neq A'$, then, by Theorems 1 and 3, there exists C_3, different from A, A', C_2 and C_2' such that AC_2C_3. By Axiom V, AC_1C_2 and AC_2C_3 imply AC_1C_3. Continue this process and obtain an infinite sequence C_1, C_2, $C_3 \cdots$. It is necessary to show that these C's are all distinct and that no two are opposites. Let us first show that AC_iC_{n+1} holds for $i = 1, 2, 3 \cdots n$. Assume it holds true for $n = k - 1$. By Axiom V, AC_iC_k and AC_kC_{k+1} imply AC_iC_{k+1}. Hence, if it holds true for $n = k - 1$, it holds true for $n = k$. But it does hold for $n = 1$. Hence our induction is complete. But, by Theorem 3, AC_iC_{n+1} implies that no C is the same as any preceding C or its opposite.

THEOREM 14. The line AB is the same as the line BA, the line $A'B$, the line $A'B'$, the line $B'A$ and the line $B'A'$.

Proof. Let X be any point of AB, to show it is also a point of the line $A'B'$. As X is on AB, $X = A$, $X = A'$, $X = B$, $X = B'$, XAB, AXB, ABX or $AX'B$. By Theorems 2 and 7, if $X = B$, then $X = (B')'$ and if $X = A$, then $X = (A')'$. By Axioms III, IV, III and IV, XAB implies $A'B'X$. By Axioms IV, III, IV, III, IV and III, AXB implies $A'X'B'$. By Axioms IV, III, IV and III, ABX implies $XA'B'$. By Axioms IV and III, Theorem 2, Axioms IV, III, IV and III, $AX'B$ implies $A'XB'$. Thus in each case X is on $A'B'$.

Similarly any point of $A'B'$ is a point of the line AB. Hence the line AB is the same as the line $A'B'$.

In like manner the line AB is the same as the line BA, the line $A'B$, the line $B'A$, and the line $B'A'$.

THEOREM 15. If a point C is on the line AB, its opposite C' is also on AB.

Proof. Suppose C is on AB. Then $C = A$, $C = B$, $C = A'$, $C = B'$, CAB, ACB, ABC or $AC'B$. By Theorem 7, if $C = A$, $C' = A'$ and if $C = B$, $C' = B'$. By Theorems 2 and 7, if $C = A'$, then $C' = A$ and if $C = B'$, then $C' = B$. By Axioms IV and III, CAB implies ABC'. By Axioms III and IV, ABC implies $C'AB$. By Theorem 2, ACB implies $A[C']'B$. Thus in each case C' is on AB.

THEOREM 16. If a point $C[A \neq C \neq A']$ is on the line AB, then B is on the line AC.

Proof. By Definition 2, C on AB implies $C = A$, $C = B$, $C = A'$, $C = B'$, CAB, ACB, ABC or $AC'B$. By hypothesis $A \neq C \neq A'$. By Theorems 2 and 7, $C = B'$ implies $B = C'$. From CAB it follows, by Axiom III, that BAC. By Axioms III, IV, III, IV and III, $AC'B$ implies $AB'C$. In each case B is on the line AC.

4. Consequences of Axioms I–V, VII.

THEOREM 17. If ABC and BCD, then D is on the line AB.

Proof. Suppose D is not on AB. Then, by Axiom VII and Theorem 10, there exists H such that CCH and DHA. But CCH is contrary to Theorem 8. Hence D is on AB.

THEOREM 18. If C and $D[C \neq D \neq C']$ are points of AB, then A is a point of CD*.

By Definition 2, C on AB implies $C = A(1)$, $C = B(2)$, $C = A'(3)$, $C = B'(4)$, $CAB(5)$, $ACB(6)$, $ABC(7)$ or $AC'B(8)$ while D on AB implies $D = A(\alpha)$, $D = B(\beta)$, $D = A'(\gamma)$, $D = B'(\delta)$, $DAB(\epsilon)$, $ADB(\zeta)$, $ABD(\eta)$,

* Cf. Axiom VI of Veblen's System, loc. cit., p. 345.

or $AD'B(\theta)$. Of the 64 conceivable cases 8[1α, 1γ, 2β, 2δ, 3α, 3γ, 4β, 4δ] are impossible.

We shall consider a few of the remaining 56 cases.

Case 5ϵ. CAB and DAB. By Axioms IV and III, DAB implies ABD'. By Theorem 17, CAB and ABD' imply that D' is on the line CA. By Theorem 15, as D' is on the line CA, its opposite D is on CA. By Theorem 16 as $D[C \neq D \neq C']$ is on the line CA, then A is on the line CD.

Case 6ζ. ACB and ADB. By Axioms III, IV and III, ACB implies CAB'. By Axioms III, IV, III, IV and III, ADB implies $AB'D'$. By Theorem 17, CAB' and $AB'D'$ imply that D' is on the line CA. By Theorem 15, as D' is on the line CA, its opposite D is on CA. By Theorem 16, as $D[C \neq D \neq C']$ is on the line CA, then A is on the line CD.

Case 7ζ. ABC and ADB. By Axiom V, ADB and ABC imply that ADC. By Axiom III, ADC implies CDA. Hence, by Definition 3, A is on CD.

By similar arguments it can be shown that in all the other cases A is on CD.

Theorem 19. If C and $D[C \neq D \neq C']$ are points of AB, then the line CD is the same as the line AB.

The proof of Theorem 19 is the same as the proof of Theorem 6 of Veblen's system.

Theorem 20. Two distinct lines can have at most a point and its opposite in common.

5. Consequences of Axioms I–VII.

Theorem 21. If KE be any line, there is a point not on KE.

Proof. Suppose KE contained all points. Then, by Axiom VI, it would contain three distinct points A, B and C such that A is not an opposite of B and such that C is not on the line AB. But, by Theorem 19, the line AB is the same as the line KE. But C is not on AB. Hence C is not on KE.

Theorem 22. If ABC and BCD and $D \neq A'$, then either ABD or $AB'D$.

Proof. By Theorem 21, there exists a point P such that P is not on the line BC. By Definition 2, it follows that P is not the opposite of B. Hence, by Theorem 1, there exists O such that BPO. From BPO it follows, by Theorem 3, that $B \neq O \neq B'$. Hence were O on the line BC, by Theorem 19, the line BO would be the same as the line BC and the point P would be on BC, contrary to assumption. Hence, by Axiom VII and Theorem 10, ABC and BPO imply the existence of E such that APE

and OEC. By Axiom VII and Theorem 10, BCD and CEO imply the existence of G such that GED and BGO.

If $G = P$ then APE and PED. From APE it follows, by Theorem 3, that $P \neq E \neq P'$. From CEO it follows, by Theorem 8 and Definition 1, that $C \neq E \neq C'$ and hence were E on BC, the line CE would be the same as the line BC and O would lie on BC, which is impossible. Hence the lines PE and BC are distinct and have in common the points A and D. From ABC and BCD it follows, by Theorem 4, that $D \neq A$. By hypothesis $D \neq A'$. But, by Theorem 20, the distinct lines PE and BC can have at most a point and its opposite in common. Hence the supposition that $G = P$ leads to a contradiction. Hence $G \neq P$.

Suppose $G = P'$. Then BPO and $BP'O$. But this is contrary to Theorem 11. Hence $P \neq G \neq P'$.

Consider the triangle AED. By Theorem 10 and Axiom VII, APE and GED imply the existence of H such that GPH and AHD. By Theorem 19, the line GP is the same as the line BO. As the line AD and the line BO have the point B in common, the lines GP and AD have in common only B and B'. Then $H = B$ or $H = B'$. Therefore ABC and BCD and $D \neq A'$ imply either ABD or $AB'D$.

THEOREM 23. If ABC and ABD and $D \neq C$, then either BCD or BDC.

Proof. By Axioms III, IV and III, ABD implies BAD'. By Axiom III, ABC implies CBA. If D' were the opposite of C, then, by Theorems 2 and 7, D would be C, contrary to hypothesis. By Theorem 22, CBA and BAD' imply that either CBD' or $CB'D'$. By Axioms III, IV and III, CBD' implies BCD. By Axioms III, IV, III and IV, $CB'D'$ implies BDC.

THEOREM 24. If ABC and ABD and $D \neq C$, then either ACD or ADC.

Proof. By Axioms III and IV, ABD implies $D'AB$. If C were the opposite of D', then, by Theorems 2 and 7, C would be D, which is contrary to hypothesis. By Theorem 22, $D'AB$ and ABC imply either $D'AC$ or $D'A'C$. By Axioms IV and III, $D'AC$ implies ACD. By Axioms IV, III and IV, $D'A'C$ implies ADC.

THEOREM 25. If ABD and ACD and $B \neq C$, then either ABC or ACB.

Proof. By Axioms III, IV and III, ABD implies BAD'. By Axioms III, IV, III, IV and III, ACD implies $AD'C'$. If C' were the opposite of B, then, by Theorems 2 and 7, C would coincide with B, contrary to hypothesis. By Theorem 22, BAD' and $AD'C'$ imply that either BAC' or $BA'C'$. By Axioms III, IV and III, BAC' implies ABC. By Axioms III, IV, III and IV, $BA'C'$ implies ACB.

THEOREM 26. If ABC is a triangle and E and F are points such that ABE and AFC, then there exists G such that FGE and BGC.

Proof. By Axioms III and IV, ABE implies $E'AB$ and hence, by Axiom III, BAE'. By Theorem 10 and Axiom VII, BAE' and AFC imply the existence of G such that BGC and $E'FG$. By Axioms IV and III, $E'FG$ implies FGE.

THEOREM 27. If ABC is a triangle and E and F are points such that AFB and AEC, then there exists D such that BCD and FED.

Proof. By Axioms III and IV, AFB implies $B'AF$. By Axioms VII and Theorem 10, $B'AF$, AEC and C not on AB (and hence not on $B'A$, by Theorem 14) imply the existence of D such that FED and $B'DC$. By Axiom IV, $B'DC$ implies BCD.

THEOREM 28. A line meeting two sides of a triangle cannot meet the third side.

Proof. Let ABC be a triangle and suppose the line l meets the side AB in F and the side AC in E. Then AFB and AEC. By Theorem 27, there exists D such that BCD and FED. From FED it follows, by Theorem 8 and Definition 1, that $F \neq E \neq F'$ and hence, by Theorem 19, that the line l is the same as the line FE. By Theorems 15 and 20, AB and BC have only B and B' in common. Hence, were F on BC, F would be either B or B'.

If $F = B$, then ABB which is contrary to Theorem 3, while if $F = B'$ then $AB'B$, contrary to Theorem 3. Hence F is not on BC.

As the distinct lines FE and BC have the point D in common, they can have only D and D' in common, by Theorems 15 and 20. Hence if l, which is the same as the line FE, meets the side BC, it must meet it in either D or D'. Hence BDC or $BD'C$.

But from BCD it follows, by Axiom III and Theorem 9, that BDC is false and, by Theorem 11 and Axioms III, IV, III, IV and III, that $BD'C$ is false.

THEOREM 29. If O is a point in the interior of the triangle ABC, then there exists Q such that AOQ and BQC.

Proof. Case I. Suppose O is between M and N where M is a point of the side AB and N is a point of the side BC. Then AMB, MON and BNC. From BNC it follows, by Theorem 8 and Definition 1, that $B \neq N \neq B'$ and hence, by Theorem 19, that the line BN is the same as the line BC. By Theorems 15 and 20, the lines AB and BN have in common only B and B'. Hence were M on BN, M would be B or B' which, by Theorem 3, is contrary to AMB. By Axiom VII, AMB, MON and M not on BN imply the existence of Q such that AOQ and BQN. By Axiom V, BQN and BNC imply BQC.

Case II. Suppose O is between M of the side AB and N of the side AC. Then AMB, MON and ANC. By Theorem 3, it follows from AMB that $M \neq B \neq M'$ and hence, by Theorem 19, that the line BM is the same as the line AB. Therefore, by Theorem 15 and 20, the lines BM and AC can have in common only A and A'. Hence were N on BM, N would be A or A', which, by Theorem 8 and Definition 1, is contrary to ANC. In like manner it follows that N is not on BC. Consider first the triangle BMN. By Axiom VII and Theorem 10, AMB and MON imply the existence of E such that BEN and AOE. Consider next the triangle BNC. By Axiom VII and Theorem 10, ANC and BEN imply the existence of Q such that AEQ and BQC. By Axiom V, AOE and AEQ imply AOQ.

THEOREM 30. A point and its opposite do not both belong to the interior of the same triangle.

Proof. Suppose P and P' are interior points of the triangle ABC. Then, by Theorem 29, there exist points E and F, such that APE, BEC, $AP'F$ and BFC. By Axioms III, IV, III, IV and III, $AP'F$ implies $AF'P$. By Theorem 20, AP and BC have in common only E and E'. Hence either F is E or F is E'.

Case I. Suppose $F = E$. Then APE and $AP'E$, which is contrary to Theorem 11.

Case II. Suppose $F = E'$. Then BEC and $BE'C$, which is contrary to Theorem 11.

THEOREM 31. If ABC is a triangle and X and F are such that AXF and BFC, then X is within the triangle ABC.

Proof. By Theorem 10, there exists E such that CEF. By Axiom III, BFC implies CFB. By Axiom V and Theorem 12, CEF and CFB imply CEB and EFB. By Theorem 3, CFB implies that $F \neq B \neq F'$ and hence, by Theorem 19, that the line BF is the same as the line BC. As A is not on BC, by hypothesis, it cannot be on BF. Consider the triangle AFB. By Axiom VII, EFB and AXF imply the existence of K such that KXE and AKB. By Definition 4, AKB, KXE and BEC imply that X is within the triangle ABC.

THEOREM 32. If X is within the triangle ABC, then X' is within the triangle $A'B'C'$.

Proof. As X is within the triangle ABC, it follows, by Theorem 29, that there exists P such that AXP and BPC. By Axioms IV, III, IV; III, IV and III, AXP and BPC imply $A'X'P'$ and $B'P'C'$ respectively. Hence, by Theorem 31, X' is within the triangle $A'B'C'$.

THEOREM 33. If O is a point collinear with 2 points M and N of a triangle ABC, the line joining O to any point $P[O \neq P \neq O']$ of a side of the triangle, meets the perimeter in a point $Q[Q \neq P]$.

THEOREM 34. If A, B and C are any three non-collinear points of the plane DEF, then the plane DEF is the same as the plane ABC.

Theorems 33 and 34 are the same as Veblen's Theorems 15 and 16. His proofs, with slight modifications for opposites, hold good here.

THEOREM 35. If two distinct non-opposite points lie in a plane, the line joining them lies in that plane.

Proof. Suppose A and B are distinct non-opposite points lying in the plane α. By Definition 5 and Theorem 19, there exists in the plane α a point C such that A, B and C are non-collinear. But, by Theorem 34, the plane ABC is the same as the plane α. The line AB is in the plane ABC. Hence AB is in α.

THEOREM 36. Every two lines in a plane intersect in two points, which are each other's opposites.

Proof. Let AB and CD be two lines in the same plane α and let us suppose they have no common point.

If B were D', then B would be on CD, contrary to the assumption that AB and CD have no common point. As $B \neq D'$ it follows, by Theorem 1, that there exists E such that DBE. From DBE it follows, by Theorem 3, that $D \neq E \neq D'$ and hence, if E were on CD, by Theorem 19, the lines DE and CD would be identical. Then B would lie on both AB and CD, contrary to our assumption concerning AB and CD. In like manner E is not on AB.

By Theorem 34, C, D and E, three non-collinear points of the plane α, determine the plane. By Theorem 33, the line AB must meet the perimeter of the triangle CED in a point $Q[Q \neq B]$.

As E is not on AB, Q cannot be E. By hypothesis, AB and CD have no common point. Hence Q cannot be C, D or a point of the side CD.

By Theorems 15 and 20, AB and ED have in common only B and B'. Hence were Q a point of the side ED, Q would be B'. But it follows from DBE, by Theorem 11 and Axiom III, that $EB'D$ is false. Hence, by Definitions 2 and 3, Q is not a point of the side ED.

Therefore Q must be a point of the side EC. By Theorem 27, EBD and EQC imply the existence of H such that BQH and DCH. By Axiom III, DCH implies HCD. By Theorem 8 and Definition 2, BQH implies $B \neq Q \neq B'$ and hence, by Theorem 19, that the line AB is the same as the line BQ. Therefore the lines AB and CD have H in common. Therefore, by Theorem 15, they have H' in common.

6. Consequences of Axioms I–IX.

THEOREM 37. If KEF be any plane, there is a point not on KEF.

Proof. Suppose the plane KEF contained all points. Then, by Axiom

* Loc. cit., page 359.

VIII, the plane would contain three non-collinear points A, B and C, and a point D such that D is not on the plane ABC. But, by Theorem 34, the plane KEF is the same as the plane ABC. But D, which is not on ABC, is not on KEF.

DEFINITION 8. A point X is *interior to the tetrahedron* $ABCD$ if it lies between two points F and G of different faces.

THEOREM 38. If a vertex A of a tetrahedron $ABCD$ be joined to an interior point O of the tetrahedron, the line AO meets the opposite face BCD in a point P such that AOP.

The proof of Theorem 38 is exactly the same as the proof of Theorem 19 of Veblen's system.*

THEOREM 39. A point and its opposite do not lie within the same tetrahedron.

Proof. Suppose the point O and its opposite O' lie within the same tetrahedron $ABCD$. By Theorem 38, there exist F and G in the face BCD such that AOF and $AO'G$. By Axioms III, IV, III, IV and III, $AO'G$ implies $AG'O$. Hence F and G are both points of the line AO. The point F must then be either G or G'. For were $F \neq G \neq F'$, the line FG would be the same as the line AO, by Theorem 19. But F and G lie in the plane BCD. Hence, by Theorem 35, every point of FG lies in the plane BCD and thus A would lie in BCD, contrary to hypothesis.

Case I. Suppose $F = G'$. Then G and G' are both within the triangle BCD, contrary to Theorem 30.

Case II. Suppose $F = G$. Then AOG and $AO'G$, contrary to Theorem 11.

THEOREM 40. If any interior point O of a tetrahedron $ABCD$ be joined to another point P of the surface or interior of the tetrahedron, the line OP meets the surface in two points Q and R such that QOR.

THEOREM 41. If O is a point in the order MNO with two points M and N of different faces of the tetrahedron $ABCD$, the line joining O to an interior point P of a face of the tetrahedron, meets the surface in Q such that $Q \neq P \neq Q'$.

THEOREM 42. If two points lie in a space $ABCD$, so does every point of the line joining them.

THEOREM 43. Any four non-coplanar points of a space, determine *that* space.

THEOREM 44. There is but one space.

THEOREM 45. If two planes have a point O in common, they have in common a second point $P[P \neq O \neq P']$.

* Loc. cit., p. 361.

Theorems 40–45 are the same as Veblen's Theorems 20–25. His proofs with slight modifications hold good here.*

THEOREM 46. Every two planes in space intersect in a straight line.

Proof. Let α and β be any two planes and let us suppose they have no common point.

Take A any point of α and B any point of β. The point B must be different from A', for otherwise B would lie on α, contrary to hypothesis. By Theorem 1, there exists C such that ABC. By Theorem 3, it follows from ABC that $A \neq C \neq A'$ and that $B \neq C \neq B'$. As the point B is not on the plane α, it follows, by Theorem 35, that C cannot be on α. In like manner C is not on β.

Take D any point in the plane β such that $D \neq B \neq D'$. The point D is not on the line CB. For were D on CB, by Theorem 16, C would be a point of BD. As B and $D(B \neq D \neq B')$ are on β every point of the line BD is on β. Hence C would lie on β, which is impossible. The points C, B, and D are non-collinear and determine a plane γ.

As the points B and C are in the plane γ, by Theorem 34, A is a point of γ. Hence the planes α and γ have one common point. Therefore, by Theorem 45, they must have a second common point E such that $A \neq E \neq A'$.

By Theorem 36, the lines EA and DB, both lying in the plane γ, must intersect in some point R. As E and A both lie in the plane α, by Theorem 33, the point R must lie in α. In like manner the point R must lie in β. As the planes α and β have one common point, by Theorem 45, they must have a second point S in common such that $S \neq R \neq S'$. By Theorem 35, the line SR lies in both α and β.

7. The Introduction of Congruence.

DEFINITION. The pairs of opposite points and the planes of space constitute a *polar system* if they are in such a reciprocal one-to-one correspondence that to the $\left\{\begin{matrix}\text{pair of opposite points}\\ \text{plane}\end{matrix}\right\}$ incident with three $\left\{\begin{matrix}\text{non-collinear planes}\\ \text{non-collinear pairs of opposite points}\end{matrix}\right\}$ corresponds the $\left\{\begin{matrix}\text{plane}\\ \text{pair of opposite points}\end{matrix}\right\}$ incident with the corresponding $\left\{\begin{matrix}\text{pairs of opposite points}\\ \text{planes}\end{matrix}\right\}$. A pair of opposite points are the *poles* of the corresponding plane, while a plane is the *polar* of its corresponding pair of opposite points. A polar system is *elliptic* if no $\left\{\begin{matrix}\text{pair of opposite points}\\ \text{plane}\end{matrix}\right\}$ is on its corresponding $\left\{\begin{matrix}\text{plane}\\ \text{pair of opposite points}\end{matrix}\right\}$.

* Loc. cit., pp. 361–363.

That our hypotheses are sufficient for the proof of the existence of elliptic polar systems can easily be verified.* Pick out a definite elliptic polar system Σ.

The segment AB is said to be congruent to the segment CD, if AB can be carried into CD by a projective transformation leaving Σ invariant.

DEFINITION. If A and B are two distinct, non-opposite points the half line AB is made up of the set of all points $[X]$ such that $X = B$, AXB or ABX.

DEFINITION. If A, B, and C are non-collinear, the boundary of the angle BAC consists of A and the half lines AB and AC.

Two angles are said to be *congruent* if they are such that the sides of one can be transformed into the sides of the other by a projective transformation leaving Σ invariant.

The usual properties of congruent segments and congruent angles can easily be deduced.†

It is now clear that the points of our space can be brought into one-to-one correspondence with the points of the hypersphere $x^2 + y^2 + z^2 + w^2 = r^2$ in such a manner that the three points A, B and C are in the order ABC, if, and only if, the corresponding points A', B' and C' on the hypersphere are such that B' is on the shorter arc of the geodesic on the hypersphere from A' to C'.

It follows that our set of axioms is categorical.

8. Questions of Independence.

Let G denote the set of Axioms I–X.

In the following E_i denotes an example of a system in which Axiom i is false but all the other Axioms of the set G are true. In every E_i use is made of a well-defined space S_i.

E_1. S_1 is a Euclidean space of three dimensions. Order has its usual significance.

E_2. S_2 consists of two points A and A'. No order exists.

E_3. S_3 consists of three points A, B and C in the orders AAC, ACC, BCA, BCC.

E_4. S_4 consists of three points A, B and C in the orders ABC and CBA.

E_5. S_5 consists of four points A, A', B and B' in the orders AAB, $A'BA$, ABA', $A'A'B$, $BA'A'$, $B'A'A'$, BAA, $B'AA$, AAB', $A'B'A$, $AB'A'$, $A'A'B'$.

E_6. S_6 consists of the points of the circumference of a circle. Three

* See J. Steiner, Synthetische Geometrie, pp. 411–414 and 422–424.

† For a set of congruence axioms for Double Elliptic Geometry of Two Dimensions see G. B. Halsted, loc. cit., pp. 217–19.

distinct points A, B and C are said to be in the order ABC, if, and only if, B is on the shorter arc from A to C.

E_7. The points of S_7 are the points on a hypersphere in space of four dimensions. Pick out a definite line l_1 and one pair of opposite points O and O' on l_1.

If the points A_1, A_2 and A_3 are not all on the line l_1, then they are said to be in the *order* $A_1A_2A_3$, if, and only if, A_2 is on the shorter arc of the geodesic from A_1 to A_3. If A_1, A_2 and A_3 are all on the line l, then they are said to be in the order $A_1A_2A_3$, if, and only if, $\bar{A}_2$ is on the shorter arc of the geodesic from $\bar{A}_1$ to $\bar{A}_3$, where (1) $\bar{A}_i$ is A_i, if A_i is neither O nor O', (2) $\bar{A}_i$ is O', if A_i is O, (3) $\bar{A}_i$ is O, if A_i is O'.

E_8. S_8 consists of the points of the surface of a sphere. Three distinct points A, B and C are said to be in the order ABC, if, and only if, B is on the shorter arc of the great circle from A to C.

E_9. S_9 is a four-dimensional double elliptic space.

E_{10}. S_{10} is Rational Three-Dimensional Double Elliptic Geometry.

UNIVERSITY OF PENNSYLVANIA.

AN APPLICATION OF A GROUP OF ORDER 16 TO A CONFIGURATION ON AN ELLIPTIC CUBIC.*

By Arnold Emch.

1. Introduction. Let P be a point on a cubic C_3, a, b two distinct tangents from P to the C_3 with the points of tangency A and B. From A let there be a line $a_{11'}$, distinct from a, intersecting the C_3 in the points 1 and 1'. Let the joins $b_{12'}$ and $b_{1'2}$ of B with 1 and 1' intersect the C_3 in 2' and 2, respectively; then, as is well known, A, 2 and 2' are on the same line $a_{22'}$. Two points A and B on a cubic are called a Steinerian† couple, when the tangents a and b at those points meet in a point of the same cubic. The cubic may now be generated by two projective quadratic pencils of lines with a self corresponding common line. Denoting this line by p and letting the letters denoting the lines also represent the left-hand sides of the linear equations of the lines, we write the equations of the two projective quadratic pencils with the parameter λ generating the cubic in the form

$$(1)\qquad \begin{aligned} m_{ab}' \cdot ap + n_{ab}' \cdot \lambda a_{11'}a_{22'} &= 0, \\ bp + \lambda b_{12'}b_{21'} &= 0, \end{aligned}$$

where m_{ab}', n_{ab}' are constant factors whose ratio is uniquely determined by the given cubic. In fact the equation of the cubic generated by (1) is

$$(2)\qquad m_{ab}' \cdot ab_{12'}b_{21'} - n_{ab}' \cdot ba_{11'}a_{22'} = 0.$$

If P is on an elliptic cubic, we can draw four tangents a, b, c, d from P to the cubic with the points of tangency A, B, C, D. With these as vertices of projective quadratic pencils of the form (1) we can generate the cubic in six different ways. Making use of the theorem‡ that a polynomial $\phi(x_1, x_2, x_3)$ contains another polynomial $\psi(x_1, x_2, x_3)$, which is irreducible, as a factor, or, except as to a constant factor, is identical with it, if ϕ vanishes for all sets of values x_1, x_2, x_3 for which ψ vanishes, from the twelve forms of the equation of the cubic resulting from those projectivities, we can establish a certain configuration of 48 lines. These are obtained from three definite ones of this configuration by the 16 substitutions of a group§ of order 16 with 15 subgroups of order 2. This group

* Read before the American Mathematical Society at Chicago, April 21, 1916.

† Clebsch-Lindemann, Vorlesungen über Geometrie, vol. I, pp. 616—— (1876).

‡ Netto, Vorlesungen über Algebra, vol. 2, theorem IX (see also X), pp. 23–24 (1900).

§ I am indebted to Prof. G. A. Miller for information concerning this group.

is represented by all couples of sets of four elements formed between the two groups of four sets each, i. e.,

1	2	3	4		1′	2′	3′	4′
2	1	4	3		2′	1′	4′	3′
3	4	1	2		3′	4′	1′	2′
4	3	2	1		4′	3′	2′	1′.

Each couple consists of two sets, one from each of these groups. All of these substitutions except the identity are of order 2. For example, from the substitution

$$S = \begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 3 & 4 & 1 & 2 & 2' & 1' & 4' & 3' \end{pmatrix}$$

we get $S^2 = 1$.

It is the purpose of this paper to establish this configuration of 48 lines explicitly by the indicated method.

2. The twelve equations representing the cubic. Let A, B, C, D be a Steinerian quadruple formed by the points of tangency of the four tangents a, b, c, d from a point P on an elliptic cubic C_3 to this cubic. Through A draw a line intersecting C_3 in the points 1 and 1′. Let the joins $b_{12'}$ and $b_{1'2}$ of B with 1 and 1′ intersect C_3 in 2′ and 2, so that their join $a_{22'}$ passes through A (Fig.). For the sake of simplicity of the construction A may be chosen as the infinite point of the C_3, without loss of generality, so that a is an asymptote. Let the joins $c_{23'}$ and $c_{2'3}$ of C with 2 and 2′ intersect C_3 in 3′ and 3. Again the join $a_{33'}$ of 3 and 3′ will pass through A. Finally let the joins $d_{24'}$ and $d_{2'4}$ of D with 2 and 2′ intersect the C_3 in 4′ and 4, so that the join $a_{44'}$ of 4 and 4′ also passes through A. From the theory of Steinerian quadruples it is well known* that the joins $b_{34'}$ and $b_{3'4}$ of B with 3 and 3′ pass through 4′ and 4; the joins $c_{14'}$ and $c_{1'4}$ of C with 1 and 1′ pass through 4′ and 4; and the joins $d_{13'}$ and $d_{1'3}$ of D with 1 and 1′ pass through 3′ and 3, respectively. From the Steinerian quadruple A, B, C, D we can choose six couples of two points each as vertices of quadratic projectivities by which the C_3 may be generated. Each of these projectivities may be written in two different forms. Thus, the projectivity with A and B as vertices, may be written in either of the forms, which we denote by $(AB)'$ and $(AB)''$ respectively, (see (1))

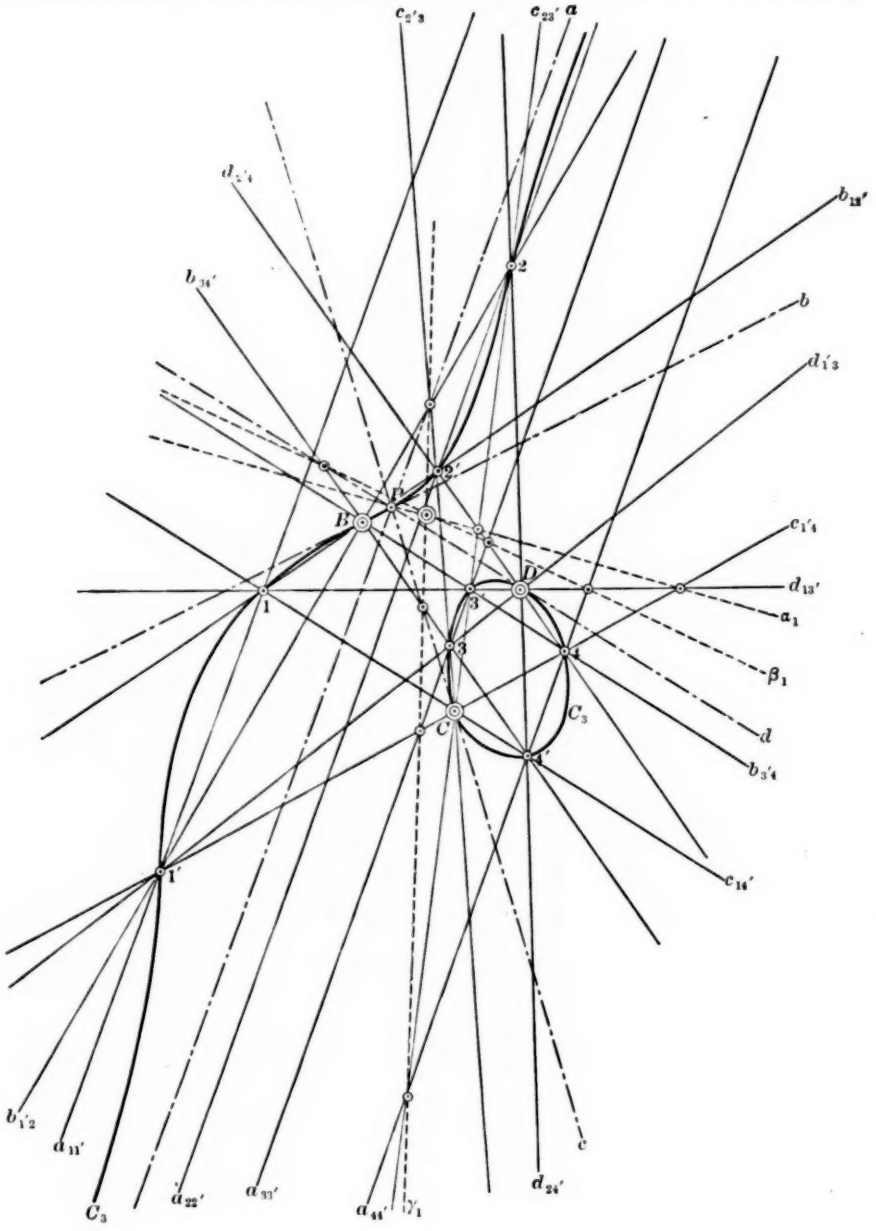
$$(4) \qquad (AB)' \begin{cases} m_{ab}' \cdot ap + n_{ab}' \cdot \lambda a_{11'} a_{22'} = 0, \\ bp + \lambda b_{12'} b_{1'2} = 0, \end{cases}$$

* Emch, Introduction to Projective Geometry, pp. 201–204.

and

$$(5) \qquad (AB)'' \begin{cases} m_{ab}'' \cdot ap + n_{ab}'' \cdot \lambda a_{33'} a_{44'} = 0, \\ bp + \lambda b_{34'} b_{43'} = 0. \end{cases}$$

Denoting the five remaining projectivities in a similar manner by $(BC)'$, $(BC)''$; $(CD)'$, $(CD)''$; etc., and forming in every case the equation gen-



erated by the projectivity, the following table of the twelve identical forms of the cubic is obtained:

$$
\begin{aligned}
(AB)' &\equiv m_{ab}' \cdot ab_{12'}b_{1'2} - n_{ab}' \cdot ba_{22'}a_{11'} = 0,\\
(AB)'' &\equiv m_{ab}'' \cdot ab_{34'}b_{3'4} - n_{ab}'' \cdot ba_{44'}a_{33'} = 0,\\
(BC)' &\equiv m_{bc}' \cdot bc_{14'}c_{2'3} - n_{bc}' \cdot cb_{34'}b_{12'} = 0,\\
(BC)'' &\equiv m_{bc}'' \cdot bc_{41'}c_{3'2} - n_{bc}'' \cdot cb_{21'}b_{43'} = 0,\\
(CD)' &\equiv m_{cd}' \cdot cd_{13'}d_{4'2} - n_{cd}' \cdot dc_{23'}c_{14'} = 0,\\
(CD)'' &\equiv m_{cd}'' \cdot cd_{31'}d_{2'4} - n_{cd}'' \cdot dc_{41'}c_{32'} = 0,\\
(AD)' &\equiv m_{ad}' \cdot ad_{31'}d_{3'1} - n_{ad}' \cdot da_{11'}a_{33'} = 0,\\
(AD)'' &\equiv m_{ad}'' \cdot ad_{24'}d_{2'4} - n_{ad}'' \cdot da_{44'}a_{22'} = 0,\\
(AC)' &\equiv m_{ac}' \cdot ac_{14'}c_{1'4} - n_{ac}' \cdot ca_{11'}a_{44'} = 0,\\
(AC)'' &\equiv m_{ac}'' \cdot ac_{32'}c_{3'2} - n_{ac}'' \cdot ca_{22'}a_{33'} = 0,\\
(BD)' &\equiv m_{bd}' \cdot bd_{13'}d_{2'4} - n_{bd}' \cdot db_{43'}b_{12'} = 0,\\
(BD)'' &\equiv m_{bd}'' \cdot bd_{24'}d_{1'3} - n_{bd}'' \cdot db_{34'}b_{21'} = 0.
\end{aligned}
\tag{6}
$$

Consider now the two equations generated by the two projectivities $(AB)'$ and $(AC)'$, characterized by the common vertex A. Writing the two equations in the form $\phi' - \psi' = 0$, $\phi'' - \psi'' = 0$, we get the equation $\phi'\psi'' - \phi''\psi' = 0$. This sextic is necessarily reducible, and contains the given C_3 as a part and some other cubic $C_3{}^*$. From the equations, $(AB)'$ and $(AC)'$, it is apparent that a and $a_{11'}$ are parts of $C_3{}^*$, so that, after dropping a and $a_{11'}$, there remains the quartic

$$(AB)'(AC)' \equiv m_{ac}'n_{ab}' \cdot ba_{22'}c_{14'}c_{1'4} - m_{ab}'n_{ac}' \cdot ca_{44'}b_{12'}b_{1'2} = 0. \tag{7}$$

By the symbol $(AB)'(AC)'$ the process is indicated by which this quartic was obtained. This quartic contains the given C_3 as a part so that the remainder is a line. From (7) it is seen that it passes through the four points of intersection of $b_{12'}$ and $c_{1'4}$ (symbolically $(b_{12'}c_{1'4})$); similarly through $(b_{1'2}c_{14'})$, $(ba_{44'})$, $(ca_{22'})$, which are not on the cubic. These four points are therefore collinear. In a similar manner we obtain eleven other quartics, each containing the given C_3 and a line, represented by the processes $(AC)'(AD)'$, $(AD)'(AB)'$, $(AB)'(AC)''$, $(AC)''(AD)''$, $(AD)''(AB)'$, $(AB)''(AC)''$, $(AC)''(AD)'$, $(AD)'(AB)''$, $(AB)''(AC)'$, $(AC)'(AD)''$, $(AD)''(AB)''$. In this manner, keeping A fixed, we obtain 12 lines. Likewise for each of the other points B, C, D of the Steinerian quadruple 12 other lines are obtained. From the three equations

$(AB)'$, $(AC)'$, $(AD)'$ in (6), and the cyclic arrangement of the processes $(AB)'(AC)'$, $(AC)'(AD)'$, $(AD)'(AB)'$ we get the three quartics:

$$(8)\quad \begin{aligned} (AB)'(AC)' &\equiv m_{ac}'n_{ab}' \cdot ba_{22'}c_{14'}c_{1'4} - m_{ab}'n_{ac}' \cdot ca_{44'}b_{12'}b_{1'2} = 0,\\ (AC)'(AD)' &\equiv m_{ad}'n_{ac}' \cdot ca_{44'}d_{13'}d_{1'3} - m_{ac}'n_{ad}' \cdot da_{33'}c_{14'}c_{1'4} = 0,\\ (AD)'(AB)' &\equiv m_{ab}'n_{ad}' \cdot da_{33'}b_{12'}b_{1'2} - m_{ad}'n_{ab}' \cdot ba_{22'}d_{13'}d_{1'3} = 0. \end{aligned}$$

When the first, second and third of these equations in the same order are multiplied by $n_{ad}' \cdot da_{33'}$, $n_{ab}' \cdot ba_{22'}$, $n_{ac}' \cdot ca_{44'}$, and added, their sum vanishes identically. Denoting the polynomial representing the given cubic C_3 by ϕ and the lines contained in the quartics (8) in the same order by the symbolic linear expressions α, β, γ, we have, after this multiplication and addition,

$$(n_{ad}' \cdot da_{33'}\alpha + n_{ab}' \cdot ba_{22'}\beta + n_{ac}' \cdot ca_{44'}\gamma)\phi \equiv 0$$

identically. But since $\phi \not\equiv 0$, we necessarily have

$$(9)\qquad n_{ad}' \cdot da_{33'}\alpha + n_{ab}' \cdot ba_{22'}\beta + n_{ac}' \cdot ca_{44'}\gamma \equiv 0.$$

From (8) it is easily seen that on each of the lines α, β, γ are four collinear points; on

$$(10)\quad \begin{aligned} \alpha&: (b_{12'}c_{1'4}),\quad (b_{1'2}c_{14'}),\quad (ba_{44'}),\quad (ca_{22'});\\ \beta&: (c_{14'}d_{1'3}),\quad (c_{1'4}d_{13'}),\quad (ca_{33'}),\quad (da_{44'});\\ \gamma&: (d_{13'}b_{1'2}),\quad (d_{1'3}b_{12'}),\quad (da_{22'}),\quad (ba_{33'}). \end{aligned}$$

In (9) the point of intersection of α and β does not lie on $a_{44'}$, since, according to (10), α cuts $a_{44'}$ in $(ba_{44'})$, and β cuts $a_{44'}$ in $(da_{44'})$. Neither does it lie on c, since α cuts c in $(ca_{22'})$, and β cuts c in $(ca_{33'})$. Hence, as (9) vanishes identically, the point of intersection of α and β must lie on γ; i. e., α, β and γ are concurrent.

It is noticed that each of the three equations represented by $(AB)'$, $(AC)'$, $(AD)'$ from which the three lines (10) were obtained had the line $a_{11'}$ in its structure. The signature $11'$ may therefore be considered as characteristic of these concurrent lines. In a similar manner, with the signatures of all other of the 16 lines, different from a, b, c, d, which with these determine the six quadratic projectivities, are associated three concurrent lines, so that altogether again the 48 lines, determined above, result.

3. Explicit representation of the configuration of the 48 lines by means of the group of order 16. Keeping in mind that to the letters a, b, c, d are attached in the same order the signatures $11'$, $22'$, $33'$, $44'$; $12'$, $1'2$, $34'$,

3′4; 14′, 1′4, 23′, 2′3; 13′, 1′3, 24′, 2′4 as subscripts, the complete table of the 48 lines is obtained by applying the 16 substitutions of the group (3) to the three lines with the signature 11′, which shall be represented by the identical substitution. In this table we write below each substitution, the signature of the three concurrent lines, the processes by which they were obtained and the four points on each of the three lines.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \end{pmatrix},$$

$$11' \begin{cases} (AB)'(AC)': & (b_{12'}c_{1'4}), & (b_{1'2}c_{14'}), & (ba_{44'}), & (ca_{22'}), \\ (AC)'(AD)': & (c_{14'}d_{1'3}), & (c_{1'4}d_{13'}), & (ca_{33'}), & (da_{44'}), \\ (AD)'(AB)': & (d_{13'}b_{1'2}), & (d_{1'3}b_{12'}), & (da_{22'}), & (ba_{33'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 2 & 1 & 4 & 3 & 2' & 1' & 4' & 3' \end{pmatrix},$$

$$22' \begin{cases} (AB)'(AC)'': & (b_{21'}c_{2'3}), & (b_{2'1}c_{23'}), & (ba_{33'}), & (ca_{11'}), \\ (AC)''(AD)'': & (c_{23'}d_{2'4}), & (c_{2'3}d_{24'}), & (ca_{44'}), & (da_{33'}), \\ (AD)''(AB)': & (d_{24'}b_{2'1}), & (d_{2'4}b_{21'}), & (da_{11'}), & (ba_{44'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 3 & 4 & 1 & 2 & 3' & 4' & 1' & 2' \end{pmatrix},$$

$$33' \begin{cases} (AB)''(AC)'': & (b_{34'}c_{3'2}), & (b_{3'4}c_{32'}), & (ba_{22'}), & (ca_{44'}), \\ (AC)''(AD)': & (c_{32'}d_{3'1}), & (c_{3'2}d_{31'}), & (ca_{11'}), & (da_{22'}), \\ (AD)'(AB)'': & (d_{31'}b_{3'4}), & (d_{3'1}b_{34'}), & (da_{44'}), & (ba_{11'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 4 & 3 & 2 & 1 & 4' & 3' & 2' & 1' \end{pmatrix},$$

$$44' \begin{cases} (AB)'(AC)': & (b_{43'}c_{4'1}), & (b_{4'3}c_{41'}), & (ba_{11'}), & (ca_{33'}), \\ (AC)'(AD)'': & (c_{41'}d_{4'2}), & (c_{4'1}d_{42'}), & (ca_{22'}), & (da_{11'}), \\ (AD)''(AB)': & (d_{42'}b_{4'3}), & (d_{4'2}b_{43'}), & (da_{33'}), & (ba_{22'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 1 & 2 & 3 & 4 & 2' & 1' & 4' & 3' \end{pmatrix},$$

$$12' \begin{cases} (BA)'(BD)': & (a_{11'}d_{2'4}), & (a_{22'}d_{13'}), & (ab_{43'}), & (db_{21'}), \\ (BD)'(BC)': & (d_{13'}c_{2'3}), & (d_{2'4}c_{14'}), & (db_{34'}), & (cb_{43'}), \\ (BC)'(BA)': & (c_{14'}a_{22'}), & (c_{2'3}a_{11'}), & (cb_{21'}), & (ab_{34'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 2 & 1 & 4 & 3 & 1' & 2' & 3' & 4' \end{pmatrix},$$

$$21' \begin{cases} (BA)'(BD)'': & (a_{22'}d_{1'3}), & (a_{1'1}d_{24'}), & (ab_{34'}), & (db_{12'}), \\ (BD)''(BC)'': & (d_{24'}c_{1'4}), & (d_{1'3}c_{23'}), & (db_{43'}), & (cb_{34'}), \\ (BC)''(BA)': & (c_{23'}a_{1'1}), & (c_{1'4}a_{22'}), & (cb_{12'}), & (ab_{43'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 3 & 4 & 1 & 2 & 4' & 3' & 2' & 1' \end{pmatrix},$$

$$34'\ \begin{cases} (BA)''(BD)': & (a_{33'}d_{4'2}), & (a_{4'4}d_{31'}), & (ab_{21'}), & (db_{43'}), \\ (BD)'(BC)': & (d_{31'}c_{4'1}), & (d_{4'2}c_{32'}), & (db_{12'}), & (cb_{21'}), \\ (BC)'(BA)'': & (c_{32'}a_{4'4}), & (c_{4'1}a_{33'}), & (cb_{43'}), & (ab_{12'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 4 & 3 & 2 & 1 & 3' & 4' & 1' & 2' \end{pmatrix},$$

$$43'\ \begin{cases} (BA)'(BD)': & (a_{44'}d_{3'1}), & (a_{3'3}d_{42'}), & (ab_{12'}), & (db_{34'}), \\ (BD)'(BC)'': & (d_{42'}c_{3'2}), & (d_{3'1}c_{41'}), & (db_{21'}), & (cb_{12'}), \\ (BC)''(BA)': & (c_{41'}a_{3'3}), & (c_{3'2}a_{44'}), & (cb_{34'}), & (ab_{21'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 1 & 2 & 3 & 4 & 4' & 3' & 2' & 1' \end{pmatrix},$$

$$14'\ \begin{cases} (CD)'(CA)': & (d_{13'}a_{4'4}), & (d_{4'2}a_{11'}), & (dc_{41'}), & (ac_{23'}), \\ (CA)'(CB)': & (a_{11'}b_{4'3}), & (a_{4'4}b_{12'}), & (ac_{32'}), & (bc_{41'}), \\ (CB)'(CD)': & (b_{12'}d_{4'2}), & (b_{4'3}d_{13'}), & (bc_{23'}), & (dc_{32'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 4 & 3 & 2 & 1 & 1' & 2' & 3' & 4' \end{pmatrix},$$

$$41'\ \begin{cases} (CD)'(CA)': & (d_{42'}a_{1'1}), & (d_{1'3}a_{44'}), & (dc_{14'}), & (ac_{32'}), \\ (CA)'(CB)'': & (a_{44'}b_{1'2}), & (a_{1'1}b_{43'}), & (ac_{23'}), & (bc_{14'}), \\ (CB)''(CD)': & (b_{43'}d_{1'3}), & (b_{1'2}d_{42'}), & (bc_{32'}), & (dc_{23'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 2 & 1 & 4 & 3 & 3' & 4' & 1' & 2' \end{pmatrix},$$

$$23'\ \begin{cases} (CD)'(CA)'': & (d_{24'}a_{3'3}), & (d_{3'1}a_{22'}), & (dc_{32'}), & (ac_{14'}), \\ (CA)''(CB)'': & (a_{22'}b_{3'4}), & (a_{3'3}b_{21'}), & (ac_{41'}), & (bc_{32'}), \\ (CB)''(CD)': & (b_{21'}d_{3'1}), & (b_{3'4}d_{24'}), & (bc_{14'}), & (dc_{41'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 3 & 4 & 1 & 2 & 2' & 1' & 4' & 3' \end{pmatrix},$$

$$32'\ \begin{cases} (CD)''(CA)'': & (d_{31'}a_{22'}), & (d_{2'4}a_{33'}), & (dc_{23'}), & (ac_{41'}), \\ (CA)''(CB)': & (a_{33'}b_{2'1}), & (a_{2'2}b_{34'}), & (ac_{14'}), & (bc_{23'}), \\ (CB)'(CD)'': & (b_{34'}d_{2'4}), & (b_{2'1}d_{31'}), & (bc_{41'}), & (dc_{14'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 1 & 2 & 3 & 4 & 3' & 4' & 1' & 2' \end{pmatrix},$$

$$13'\ \begin{cases} (DC)'(DB)': & (c_{14'}b_{3'4}), & (c_{3'2}b_{12'}), & (cd_{42'}), & (bd_{24'}), \\ (DB)'(DA)': & (b_{12'}a_{3'3}), & (b_{3'4}a_{11'}), & (bd_{31'}), & (ad_{42'}), \\ (DA)'(DC)': & (a_{11'}c_{3'2}), & (a_{3'3}c_{14'}), & (ad_{24'}), & (cd_{31'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 3 & 4 & 1 & 2 & 1' & 2' & 3' & 4' \end{pmatrix},$$

$$31' \begin{cases} (DC)''(DB)'': & (c_{32'}b_{1'2}), & (c_{1'4}b_{34'}), & (cd_{24'}), & (bd_{42'}), \\ (DB)''(DA)': & (b_{34'}a_{1'1}), & (b_{1'2}a_{33'}), & (bd_{13'}), & (ad_{24'}), \\ (DA)'(DC)'': & (a_{33'}c_{1'4}), & (a_{1'1}c_{32'}), & (ad_{42'}), & (cd_{13'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 2 & 1 & 4 & 3 & 4' & 3' & 2' & 1' \end{pmatrix},$$

$$24' \begin{cases} (DC)'(DB)'': & (c_{23'}b_{4'3}), & (c_{4'1}b_{21'}), & (cd_{31'}), & (bd_{13'}), \\ (DB)''(DA)'': & (b_{21'}a_{4'4}), & (b_{4'3}a_{22'}), & (bd_{42'}), & (ad_{31'}), \\ (DA)''(DC)': & (a_{22'}c_{4'1}), & (a_{4'4}c_{23'}), & (ad_{13'}), & (cd_{42'}); \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 1' & 2' & 3' & 4' \\ 4 & 3 & 2 & 1 & 2' & 1' & 4' & 3' \end{pmatrix},$$

$$42' \begin{cases} (DC)''(DB)': & (c_{41'}b_{2'1}), & (c_{2'3}b_{43'}), & (cd_{13'}), & (bd_{31'}), \\ (DB)'(DA)'': & (b_{43'}a_{2'2}), & (b_{2'1}a_{44'}), & (bd_{24'}), & (ad_{13'}), \\ (DA)''(DC)': & (a_{44'}c_{2'3}), & (a_{2'2}c_{41'}), & (ad_{31'}), & (cd_{24'}); \end{cases}$$

4. Discussion of the configuration. The foregoing table contains 96 distinct points through which the 48 lines pass. Through each of these points two of the lines pass. The 48 lines in 16 sets of three are concurrent, so that they pass through 16 other fixed points in triplets. Of the 96 points 48 are formed by intersections of the 16 lines forming the projectivities. The other 48 points are formed by the intersections of the tangents a, b, c, d with the same 16 lines. In the figure only one of the sixteen sets of concurrent lines is shown; it corresponds to the set with the signature 43′ and the three lines are denoted by $\alpha_1, \beta_1, \gamma_1$. The remaining fifteen sets may also be constructed without difficulty. They have been omitted in order not to overload the figure.

UNIVERSITY OF ILLINOIS.

THE NUMERICAL FACTORS OF THE ARITHMETIC FORMS $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$.

By Tracy A. Pierce.

1. Introduction. The object of the present investigation is to study the arithmetic properties of the numbers given by the forms $\Pi_{i=1}^{n}(1 \pm \alpha_i^m)$ where $\alpha_1, \alpha_2, \cdots, \alpha_i, \cdots, \alpha_n$ are the roots of the equation

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0, \tag{1}$$

whose coefficients are integers. It is readily seen that $\Pi_{i=1}^{n}(1 \pm \alpha_i^m)$ represents an integer, for since it is a rational integral symmetric function of the roots of (1) it may be rationally and integrally expressed in terms of the integer coefficients of (1).

As m takes different positive integer values the forms $\Pi_{i=1}^{n}(1 - \alpha_i^m)$ and $\Pi_{i=1}^{n}(1 + \alpha_i^m)$ generate two series of integers. The numbers of these series will be designated by Δ_m and S_m respectively.

Using different arithmetic forms, namely $(\alpha^m - \beta^m)/(\alpha - \beta)$ and $\alpha^m + \beta^m$, Lucas* and Carmichael† have done work of a somewhat similar character but for the case of a quadratic equation only. The properties of Δ_m and S_m which depend on the principles of algebraic divisibility are almost identical with the corresponding properties of the forms used by Lucas and Carmichael. In § 2 we develop these properties of Δ_m and S_m.

In § 3 by the use of the dialytic method of elimination applied to congruences a condition for real solutions of $f(x) \equiv 0 \pmod{p}$ is obtained. The condition is expressed in terms of Δ_{p-1} calculated for the equation $f(x) = 0$.

In § 4 we investigate the factors of Δ_m corresponding to real solutions of $f(x) \equiv 0 \pmod{p^m}$.

In §§ 5, 6, and 7 algebraic number-theory is applied to determine the forms of the factors of Δ_p. The cases of the quadratic, cubic, and the general equation are treated separately.

In § 8 the forms of the factors of Δ_m where m is composite are determined.

---

* Am. Journ. of Math., vols. 1 and 2, 1878–79.

† Annals of Math., Second Series, vol. 15 (1913) p. 30. References to other works are given in this paper as well as in the Encyk. der Math. Wiss., 1:2, p. 596.

2. **Properties of Δ_m and S_m depending on algebraic divisibility.** Since

$$\prod_{i=1}^{n}(1-\alpha_i^{2m}) = \prod_{i=1}^{n}(1+\alpha_i^{m})\prod_{i=1}^{n}(1-\alpha_i^{m}),$$

$$\Delta_{2m} = S_m \cdot \Delta_m. \tag{2}$$

Continued application of this decomposition gives

$$\Delta_{2^\lambda k} = S_{2^{\lambda-1}k} \cdot S_{2^{\lambda-2}k} \cdots S_k \cdot \Delta_k.$$

Also since

$$\frac{\Delta_{md}}{\Delta_d} = \frac{\prod_{i=1}^{n}(1-\alpha_i^{md})}{\prod_{i=1}^{n}(1-\alpha_i^{d})} = \prod_{i=1}^{n}(1+\alpha_i^{d}+\alpha_i^{2d}+\cdots+\alpha_i^{(m-1)d})$$

is a rational integral symmetric function of the roots of (1) it is an integer and therefore Δ_{md} is divisible by Δ_d and similarly by Δ_m. Hence in general the Δ's of composite subscript are factorable immediately.

As a particular case of the result above, every Δ_m is divisible by

$$\Delta_1 = \prod_{i=1}^{n}(1-\alpha_i) = 1 - \Sigma\alpha_i + \Sigma\alpha_i\alpha_j - \cdots \pm \Pi\alpha_i$$
$$= 1 + a_1 + a_2 + \cdots + a_n.$$

Or, in other words, every Δ_m is divisible by the sum of the coefficients of equation (1).

In as much as

$$\frac{S_{(2m+1)d}}{S_d} = \frac{\prod_{i=1}^{n}(1+\alpha_i^{(2m+1)d})}{\prod_{i=1}^{n}(1+\alpha_i^{d})} = \prod_{i=1}^{n}(1-\alpha_i^{d}+\alpha_i^{2d}-\cdots\pm\alpha_i^{2md})$$

is a rational integral symmetric function of the roots of (1) we see that $S_{(2m+1)d}$ is divisible by S_d. In particular, every S_m whose subscript is odd is divisible by

$$S_1 = \prod_{i=1}^{n}(1+\alpha_i) = 1 + \Sigma\alpha_i + \Sigma\alpha_i\alpha_j + \cdots + \Pi\alpha_i$$
$$= 1 - a_1 + a_2 - \cdots \pm a_n.$$

We shall now develop formulæ for partially factoring Δ_m and S_m. To this end let $Q_m(x) = 0$ be the algebraic equation, with leading coefficient unity, whose roots are the primitive mth roots of unity; then

$$x^m - 1 = \prod_d Q_d(x),$$

where d ranges over all the divisors of m.*

* Bachmann, Kreistheilung, 3d lecture.

By means of the equation above we may express Δ_m in terms of the Q-function. Thus, we have

$$\pm \Delta_m = \prod_{i=1}^{n}(1 - \alpha_i^m) = \prod_{i=1}^{n}\prod_{d} Q_d(\alpha_i) = \prod_{d}\prod_{i=1}^{n} Q_d(\alpha_i). \tag{3}$$

For any particular divisor d_1 of m we see that $\Pi_{i=1}^{n} Q_{d_1}(\alpha_i)$ is an integer; hence (3) gives a partial arithmetic factorization of Δ_m when m is composite.

The corresponding factorization of S_m may be obtained as follows. Since

$$\pm \Delta_m = \prod_{i=1}^{n}\prod_{d} Q_d(\alpha_i),$$

d running over all divisors of m, and

$$\pm \Delta_{m/v} = \prod_{i=1}^{n}\prod_{d'} Q_{d'}(\alpha_i),$$

d' running over all divisors of m/v, it follows that

$$\pm \frac{\Delta_m}{\Delta_{m/v}} = \prod_{i=1}^{n}\prod_{\delta} Q_\delta(\alpha_i),$$

where δ ranges over all the divisors of m which are not at the same time divisors of m/v. Now replace m by $2m$ and give v the value 2; then we have by means of (2)

$$\pm \frac{\Delta_{2m}}{\Delta_m} = \pm S_m = \prod_{i=1}^{n}\prod_{\delta} Q_\delta(\alpha_i),$$

where δ ranges over those divisors of $2m$ which contain 2 to the same power as $2m$ itself. This last formula furnishes the partial factorization of S_m when m is composite.

It is a property of the Q-function that

$$Q_m(x) = \frac{(x^m - 1)\Pi(x^{m/p_ip_j} - 1)\cdots}{\Pi(x^{m/p_i} - 1)\Pi(x^{m/p_ip_jp_k} - 1)\cdots}.$$

By substituting $\alpha_1, \alpha_2, \cdots, \alpha_n$ successively for x in this equation and multiplying together the corresponding members of the resulting equations we obtain

$$\prod_{i=1}^{n} Q_m(\alpha_i) = \pm \frac{\Delta_m \Pi \Delta_{m/p_ip_j}\cdots}{\Pi\Delta_{m/p_i}\Pi\Delta_{m/p_ip_jp_k}\cdots}, \tag{4}$$

where the factors denoted by Π in the right-hand member extend over the combinations 2, 4, 6, $\cdots$ at a time of the prime factors $p_i, p_j, p_k, \cdots$ of m in the numerator and over the combinations 1, 3, 5, $\cdots$ at a time in the denominator.

Now if d is a divisor of m we have by means of (3) and (4),

$$\pm \Delta_m = \prod_d \prod_{i=1}^{n} Q_d(\alpha_i) = \pm \prod_d \frac{\Delta_d \Pi \Delta_{d/p_i p_j} \cdots}{\Pi \Delta_{d/p_i} \Pi \Delta_{d/p_i p_j p_k} \cdots},$$

the product extending over all divisors d of m, the p's being the prime factors of d for each d. The corresponding formula for S_m is

$$\pm S_m = \prod_\delta \prod_{i=1}^{n} Q_\delta(\alpha_i) = \pm \prod_\delta \frac{\Delta_\delta \Pi \Delta_{\delta/p_i p_j} \cdots}{\Pi \Delta_{\delta/p_i} \Pi \Delta_{\delta/p_i p_j p_k} \cdots},$$

where δ ranges over those divisors of $2m$ which contain 2 to the same power as $2m$ itself, and the p's are the prime factors of δ for each δ.

In consideration of equation (3) we may state the following theorem:

If $m_1, m_2, \cdots, m_s$ and $n_1, n_2, \cdots, n_r$ be two sets of positive integers such that any positive integer d which is a factor of just t integers of the second set is also a factor of at least t integers of the first set, then the number

$$\frac{\Delta_{m_1} \cdot \Delta_{m_2} \cdots \Delta_{m_s}}{\Delta_{n_1} \cdot \Delta_{n_2} \cdots \Delta_{n_r}}$$

is an integer.

*It follows that the product of any n consecutive terms of the series of numbers $\Delta_1, \Delta_2, \Delta_3, \cdots$ is divisible by the product of the first n terms.**

The corresponding theorems for the series $S_1, S_2, S_3, \cdots$ are:

If $m_1, m_2, m_3, \cdots, m_s$ and $n_1, n_2, n_3, \cdots, n_r$ be two sets of positive integers such that every positive integer d which is a factor of just t integers of the second set with odd quotient is a factor of at least t integers of the first set with odd quotient, then the number

$$\frac{S_{m_1} \cdot S_{m_2} \cdots S_{m_s}}{S_{n_1} \cdot S_{n_2} \cdots S_{n_r}}$$

is an integer.

The product of any $2n - 1$ consecutive terms of the series $S_1, S_2, S_3, \cdots$ is divisible by the product of the first n terms.

3. **Condition for real solutions of $f(x) \equiv 0 \pmod{p}$.** The factors of the Δ's furnish valuable information concerning the existence of real solutions of the congruence

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n \equiv 0 \pmod{p} \qquad (5)$$

whose left-hand member is the left-hand member of equation (1) and whose modulus is an odd prime p ($p > n$). Indeed we may consider in connection with the above congruence the following

$$x^{\phi(p)} - 1 \equiv 0 \pmod{p},$$

* Compare the corresponding theorems in Carmichael's and Lucas's works (already cited).

where φ is the ordinary totient function. It is well known that this last congruence has its full complement of real roots. If congruence (5) be multiplied by $x, x^2, \cdots, x^{\phi(p)}$ successively and reduced each time by means of the second congruence we shall obtain $\varphi(p)$ congruences. Now regarding the various powers of x as indeterminates of the first degree a necessary condition that the $\varphi(p)$ linear congruences be consistent, and consequently that congruence (5) have a real solution, is that

$$\begin{vmatrix} 1, & a_1, & a_2, & \cdots, & a_n, & 0, & \cdots, & 0 \\ 0, & 1, & a_1, & \cdots, & a_{n-1}, & a_n, & \cdots, & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ a_1, & a_2, & a_3, & \cdots, & 0, & 0, & \cdots, & 1 \end{vmatrix} \equiv 0 \pmod{p}$$

where the determinant is formed so that the elements in the leading diagonal are unity and the other elements in each row are formed from the $p-1$ quantities $1, a_1, \cdots, a_n, 0, \cdots, 0$ in cyclical order.

This circulant-determinant of order $\varphi(p) = p - 1$ is known* to be equal to the product

$$f(r_1) \cdot f(r_2) \cdots f(r_{p-1}),$$

where $r_1, r_2, \cdots, r_{p-1}$ are the roots of the equation $x^{p-1} - 1 = 0$. The last product, from the properties of algebraic resultants, is equal numerically to

$$\prod_{i=1}^{n}(1 - \alpha_i^{p-1}) = \Delta_{p-1}.$$

Hence a necessary condition that $f(x) \equiv 0 \pmod{p}$ *shall have a real solution is that* $\Delta_{p-1} \equiv 0 \pmod{p}$, *or that* Δ_{p-1} *be divisible by* p. Conversely it is not difficult to prove that if $f(x) \equiv 0 \pmod{p}$ has a real root then $\Delta_{p-1} \equiv 0 \pmod{p}$.

If equation (1) has as one of its roots an rth root of unity, then

$$\Delta_r = \prod_{i=1}^{n}(1 - \alpha_i^r) = 0$$

and also

$$\Delta_{rk} = 0.$$

By the results of the preceding paragraph, the congruence $f(x) \equiv 0 \pmod{p}$ has in this case a real solution for every prime of the form $rk + 1$.

We shall exclude from further consideration the special case when equation (1) has among its roots any root of unity. We shall also assume that (1) is irreducible in the field of rational integers.

* Scott: Theory of Determinants, p. 81.

4. **Properties of the Δ's depending on real solutions of $f(x) \equiv 0 \pmod p$.** If we form the equation whose roots are the mth powers of the roots of equation (1) and, following the notation of Gauss, designate this equation by $(f, \alpha^m) = 0$ we have

$$(f, \alpha^m) = \Pi(x - \alpha_i^m) = x^n - \Sigma\alpha_i^m x^{n-1} + \Sigma\alpha_i^m\alpha_j^m x^{n-2} - \cdots \pm \Pi\alpha_i^m$$

and

$$(f, \alpha^m)_{x=1} = \Pi(1 - \alpha_i^m) = 1 - \Sigma\alpha_i^m + \Sigma\alpha_i^m\alpha_j^m - \cdots \pm \Pi\alpha_i^m = \Delta_m. \quad (6)$$

Now it is easy to see that if the original congruence $(f, \alpha) \equiv 0 \pmod p$ has the solution $x \equiv k \pmod p$ then the congruence $(f, \alpha^m) \equiv 0 \pmod p$ has the solution $x \equiv k^m \pmod p$. For since $(f, \alpha) = \Pi(x - \alpha_i)$ and $(f, \alpha^m) = \Pi(x - \alpha_i^m)$ it follows that if $\Pi(k - \alpha_i) \equiv 0 \pmod p$ then $\Pi(k^m - \alpha_i^m) \equiv 0 \pmod p$; for $\Pi(k^m - \alpha_i^m)$ is algebraically divisible by $\Pi(k - \alpha_i)$ which is itself a multiple of p by hypothesis.

It follows that if k belongs to the exponent e modulo p then $x \equiv k^e \equiv 1 \pmod p$ is a solution of $(f, \alpha^e) \equiv 0 \pmod p$; whence by means of (6) we see that Δ_e is divisible by p.

The S's may be treated in a similar manner by use of the equation

$$(f, \alpha^m)_{x=-1} = \pm (1 + \Sigma\alpha_i^m + \cdots + \Pi\alpha_i^m) = \pm \Pi(1 + \alpha_i^m) = \pm S_m.$$

Thus whenever Δ_{p-1} is divisible by p and $x \equiv k \pmod p$ is a solution of $(f, \alpha) \equiv 0 \pmod p$ such that $k^{e_1} \equiv -1 \pmod p$ then $(f, \alpha^{e_1}) \equiv 0 \pmod p$ has the solution $x \equiv -1 \pmod p$, or in other words S_{e_1} is divisible by p. If the exponent e to which k belongs modulo p is even, then $k^{e/2} \equiv -1 \pmod p$.* Furthermore if $k^e \equiv 1 \pmod p$ then assuming e less than $p - 1$ we have $e \leqq \frac{1}{2}(p - 1)$. In view of this fact, we may state the theorem: *If in the sequence* $\Delta_1, \Delta_2, \cdots, \Delta_{\frac{1}{2}(p-1)}, S_1, S_2, \cdots, S_{\frac{1}{2}(p-1)}$ *the prime* p *appears only as a factor of* $S_{\frac{1}{2}(p-1)}$ *then the real solution of* $(f, \alpha) \equiv 0 \pmod p$ *is a primitive root of* p.

When the congruence $(f, \alpha) = \Pi(x - \alpha_i) \equiv 0 \pmod p$ has m incongruent solutions $k_1, k_2, \cdots, k_m$ and no multiple solutions, thus implying that p does not divide the discriminant of $(f, \alpha) = 0$, the congruence

$$(f, \alpha) \equiv 0 \pmod{p^m}$$

also has m solutions $K_1, K_2, \cdots, K_m$ all of which are distinct.† Thus if

$$(f, \alpha) \equiv (x - k_1)(x - k_2) \cdots (x - k_m)\psi(x) \pmod p \quad (7)$$

then

$$(f, \alpha) \equiv (x - K_1)(x - K_2) \cdots (x - K_m)\Psi(x) \pmod{p^m}. \quad (8)$$

Furthermore if this last congruence holds, then

* Wertheim: Elemente der Zahlentheorie, Lehrsatz II, p. 124.

† H. J. S. Smith: Report on the Theory of Numbers, Collected Math. Papers, Vol. I, p. 157.

$(f, \alpha^{p-1}) \equiv (x - K_1{}^{p-1})(x - K_2{}^{p-1}) \cdots (x - K_m{}^{p-1})\Phi(x) \pmod{p^m}$; (9)
for if K is a root of $(f, \alpha) = \Pi(x - \alpha_i) \equiv 0 \pmod{M}$ then K^l is a root of $(f, \alpha^l) = \Pi(x - \alpha_i{}^l) \equiv 0 \pmod{M}$ because $\Pi(K^l - \alpha_i{}^l)$ is a multiple of $\Pi(K - \alpha_i)$ which is itself a multiple of M. From (6) and (9) we see that $\Delta_{p-1} = (f, \alpha^{p-1})_{x=1} \equiv (1 - K_1{}^{p-1})(1 - K_2{}^{p-1}) \cdots (1 - K_m{}^{p-1})\Phi(1) \pmod{p^m}$. Since each factor on the right except $\Phi(1)$ is divisible by at least the first power of p, it follows that

$$\Delta_{p-1} \equiv 0 \pmod{p^m}.$$

If m_1 of the roots K_i belong to the exponent e modulo p then $\Delta_e \equiv 0 \pmod{p^{m_1}}$, and if m_2 of the roots are such that $K^{e_1} \equiv -1 \pmod{p}$ then $S_{e_1} \equiv 0 \pmod{p^{m_2}}$.

5. **Forms of the Factors of Δ_q for the Quadratic Equation.** As already noted a Δ_m of composite subscript m is divisible by Δ_d where d is a divisor of m. In this section we shall discuss the factors of Δ_q where q is a prime.

We are able to determine the exact forms of the factors of Δ_q for the case when (1) is a quadratic equation. In other cases we may set up tentative methods whereby the factors are readily found. The case of the quadratic equation will first be considered.

Equation (1) is then an irreducible equation of the form

$$x^2 + a_1 x + a_2 = 0. \tag{10}$$

A root of this equation generates a quadratic number field which is indeed a Galois field.* In this field the rational primes, exception being made of those which divide the discriminant of (10), separate into two classes according as the congruence

$$x^2 + a_1 x + a_2 \equiv 0 \pmod{p}, \tag{11}$$

where p is the prime in question, has or has not real solutions. If the prime p belongs to the first class it will decompose in the quadratic number field into the product of two prime ideals whose norms are the original prime p. Thus if $(p) = \mathfrak{p}_1\mathfrak{p}_2$ then $n(\mathfrak{p}_1) = p$, $n(\mathfrak{p}_2) = p$ and also $\varphi(\mathfrak{p}_1) = p - 1$ where φ is the totient function in the quadratic field. If the prime p belongs to the second class then the ideal (p) is a prime ideal not decomposable in the field and $n(p) = p^2$, $\varphi(p) = p^2 - 1$.

If the roots of (10) are α_1 and α_2 Fermat's theorem for a prime ideal $\mathfrak{p}_1$ which divides (p), where p is a rational prime of the first class, gives

$$\alpha_1{}^{(p-1)} - 1 \equiv 0 \pmod{\mathfrak{p}_1},$$
$$\alpha_2{}^{(p-1)} - 1 \equiv 0 \pmod{\mathfrak{p}_2}.$$

* Hilbert: Jahresbericht der Deutsch. Math. Vereinigung, Vol. 4, 1894–95, Kapitel XVI.

The second modulus may be changed to $\mathfrak{p}_1$ since the conjugate fields are identical in a Galois field. Then since $\alpha_1^{p-1} - 1$ and $\alpha_2^{p-1} - 1$ are both numbers of the ideal $\mathfrak{p}_1$ their product $\Pi_{i=1,\ 2}(1 - \alpha_i^{p-1}) = \Delta_{p-1}$ is also a number of $\mathfrak{p}_1$. Now it is known that all rational numbers of $\mathfrak{p}_1$ are multiples* of the rational prime p and since Δ_{p-1} is a rational number of $\mathfrak{p}_1$ we may write in the ordinary sense of a congruence,

$$\Delta_{p-1} \equiv 0 \pmod{p}.$$

It is necessary now to see that the conjugate numbers α_1 and α_2 belong to the same exponent modulo the corresponding conjugate ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively. Indeed one conjugate ideal is constructed from the other by simply substituting conjugate numbers. Hence, if $\alpha_1^e \equiv 1 \pmod{\mathfrak{p}_1}$, where e is the smallest exponent for which this occurs, then $\alpha_2^e \equiv 1 \pmod{\mathfrak{p}_2}$ and we could not have $\alpha_2^{e_1} \equiv 1 \pmod{\mathfrak{p}_2}$ where $e_1 < e$ for if so we could pass back to $\mathfrak{p}_1$ by substituting α_1 for α_2 and we should have $\alpha_1^{e_1} \equiv 1 \pmod{\mathfrak{p}_1}$ contrary to hypothesis.

Since the theory of power residues for an algebraic number field is precisely similar to the ordinary theory† we see that the prime p (when not a factor of Δ_1) can only appear as a factor of those Δ's having prime subscripts for which the subscripts are divisors of $p - 1$. In particular if p is not a factor of Δ_1 but is a factor of Δ_q, where q is a prime, then $k'q = p - 1$ and therefore

$$p = k'q + 1. \tag{12}$$

Similarly for a prime p of the second class $\Delta_{p^2-1} \equiv 0 \pmod{p}$. If p is not a factor of Δ_1 but is a factor of Δ_q where q is a prime then q must divide $p^2 - 1 = (p - 1)(p + 1)$. Now q cannot divide $p - 1$, for then Δ_{p-1} would be divisible by p and congruence (11) would be solvable, which is not the case for primes of the second class. Hence q must divide $p + 1$ and therefore $kq = p + 1$. Hence $p = kq - 1$.

Combining this result with that of (12) *we see that if q is a prime number the prime factors of* Δ_q, *other than those which divide* Δ_1 *or the discriminant of* (10), *are of the forms* $kq \pm 1$.

It is remarkable to note that $-\Delta_q$ calculated for the particular quadratic equation $x^2 - 2 = 0$ is the number $2^q - 1$ and hence that the Mersenne numbers $2^q - 1$ are included among the Δ's of this equation. Similarly $-\Delta_q$ of the equation $x^2 - a = 0$ is a number of the form $a^q - 1$. The methods of factorization given above may then be applied to numbers of these forms.

6. **Forms of the factors of Δ_q for a cubic equation.** A similar situ-

* Sommer: Vorlesungen ueber Zahlentheorie, p. 59.

† Hilbert: l. c., Kapitel III, § 9.

ation to that of a quadratic equation arises when (1) is a cubic or higher degree equation. The problem here must be treated somewhat differently since here the conjugate number fields are not in general identical.

If we consider the irreducible cubic equation

$$x^3 + a_1x^2 + a_2x + a_3 = 0, \tag{13}$$

each of the roots α_1, α_2, and α_3 generates a cubic number field. The three fields thus generated are conjugate. Between these fields there is a one-to-one correspondence of ideals, the ideals of one field being obtained from those of another by substituting for the numbers of the latter the corresponding conjugate numbers of the former.* Furthermore, if $\mathfrak{a}_1$, $\mathfrak{a}_2$, and $\mathfrak{a}_3$, be three conjugate ideals the norm of each is equal to the product $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \mathfrak{a}_3$, which is a principal ideal all of whose numbers are multiples of a rational integer.

The rational primes in this cubic field, other than the prime factors of the discriminant of (13), separate into three classes according as the congruence

$$x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}, \tag{14}$$

whose modulus is the prime in question, has three real solutions, one real solution, or no real solution.†

Considering p to be a prime of the first class it decomposes in each of the three conjugate fields into the product of three prime ideals all of whose norms are equal to p. Thus

$$(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3, \qquad (p) = \mathfrak{p}_1'\mathfrak{p}_2'\mathfrak{p}_3', \qquad (p) = \mathfrak{p}_1''\mathfrak{p}_2''\mathfrak{p}_3'',$$
$$n(\mathfrak{p}_1) = n(\mathfrak{p}_2) = n(\mathfrak{p}_3) = n(\mathfrak{p}_1') = \text{etc.} = p,$$

$$\varphi(\mathfrak{p}_1) = n(\mathfrak{p}_1)\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right) = p - 1, \qquad \varphi(\mathfrak{p}_2) = \varphi(\mathfrak{p}_3) = \varphi(\mathfrak{p}_1') = \text{etc.} = p - 1.$$

By Fermat's theorem

$$\alpha_1^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}_1},$$
$$\alpha_2^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}_1'},$$
$$\alpha_3^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}_1''}.$$

Multiplying the left-hand members together gives a number $\Pi_{i=1}^{3}(1-\alpha_i^{p-1}) = \Delta_{p-1}$, which belongs to an ideal which is the product of the three moduli, namely $\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1'' = n(\mathfrak{p}_1) = p$. Hence

$$\Delta_{p-1} \equiv 0 \pmod{p}. \tag{15}$$

Consideration of the ideals $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_2''$ and also of $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_3''$ yields congruence (15) again in both cases.

* Hilbert: l. c., p. 191.

† Sommer: l. c., §§ 44–46.

If the prime p is of the second class, then

$$(p) = \mathfrak{p}_1\mathfrak{p}_2, \quad (p) = \mathfrak{p}_1'\mathfrak{p}_2', \quad (p) = \mathfrak{p}_1''\mathfrak{p}_2'',$$
$$n(\mathfrak{p}_1) = n(\mathfrak{p}_1') = n(\mathfrak{p}_1'') = p, \qquad n(\mathfrak{p}_2) = n(\mathfrak{p}_2') = n(\mathfrak{p}_2'') = p^2,$$
$$\varphi(\mathfrak{p}_1) = \varphi(\mathfrak{p}_1') = \varphi(\mathfrak{p}_1'') = p - 1, \qquad \varphi(\mathfrak{p}_2) = \varphi(\mathfrak{p}_2') = \varphi(\mathfrak{p}_2'') = p^2 - 1.$$

Just as in the two preceding paragraphs the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_1'$, $\mathfrak{p}_1''$ yield congruence (15) again, but for $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_2''$ we have

$$\alpha_1^{p^2-1} - 1 \equiv 0 \pmod{\mathfrak{p}_2},$$
$$\alpha_2^{p^2-1} - 1 \equiv 0 \pmod{\mathfrak{p}_2'},$$
$$\alpha_2^{p^2-1} - 1 \equiv 0 \pmod{\mathfrak{p}_2''}.$$

Multiplying together the left-hand members we see that Δ_{p^2-1} must be a number of the ideal $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2'' = n(\mathfrak{p}_2) = p^2$, hence

$$\Delta_{p^2-1} \equiv 0 \pmod{p^2}. \tag{16}$$

Finally if p be a prime number of the third class the congruence (14) is not solvable and p is not decomposable in the conjugate fields and is itself a principal ideal of these fields. The norm of (p) is p^3. Then

$$\alpha_1^{p^3-1} - 1 \equiv 0 \pmod{(p)},$$
$$\alpha_2^{p^3-1} - 1 \equiv 0 \pmod{(p)},$$
$$\alpha_3^{p^3-1} - 1 \equiv 0 \pmod{(p)},$$

and hence

$$\Delta_{p^3-1} \equiv 0 \pmod{p^3}. \tag{17}$$

In view of (15), (16), and (17) we see that if a prime p, which does not divide Δ_1 or the discriminant of (13), enters Δ_q as a factor, where q is a prime, then q must divide either $p - 1$, $p^2 - 1$, or $p^3 - 1$. *Thus* $kq + 1$ *equals either* p, p^2, *or* p^3.

When testing for prime factors of Δ, we form the even multiples of q, add unity and use as trial divisors those primes p for which $2kq + 1$ equals either p, p^2, or p^3.

The upper limit to which the form $2kq + 1$ must be calculated may be determined as follows. If a prime p_1 is a factor of Δ_q (and not a factor of Δ_1 since Δ_1 is a factor of every Δ_m), then p_1 will enter Δ_q in the first, second, or third power according as p_1 is of the first, second, or third class, and p_1 raised to the power in which it occurs will be of the form $2kq + 1$. The same will be true of a second prime which enters Δ_q. Thus $\Delta_q \div \Delta_1$ will have a decomposition such as $p_1p_2^2p_3^3p_4^2 \cdots$ where each factor as printed will be of the form $2kq + 1$. At least one of these factors will be less than the square root of $\Delta_q \div \Delta_1$, hence we calculate the values of $2kq + 1$ only as far as the square root of $\Delta_q \div \Delta_1$. We must also assure ourselves that $\Delta_q \div \Delta_1$ is not the square or the cube of a single prime.

As an illustration $\Delta_{61} \div \Delta_1$ calculated for the equation $x^3 + x + 1 = 0$ is equal to 4459734401. We form the values of $2k \cdot 61 + 1$ less than the square root of the number in question and according to the above criterion have 113 trial divisions to make. Since none of these divisions are exact we know that 4459734401 is a prime number. If we tested as trial divisors all primes less than the square root of the number above we should have to make 6,675 trials.

7. **Forms of the factors of Δ_q for the general equation.** Returning now to the general equation (1), namely,

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0 \tag{1}$$

it is known* that when

$$f(x) \equiv P_1^{e_1}(x)P_2^{e_2}(x) \cdots P_r^{e_r}(x) \pmod{p}, \tag{18}$$

where $P_1(x), \cdots, P_r(x)$ are prime functions of degrees $f_1, f_2, \cdots, f_r$, then p in the field generated by α has the decomposition

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}, \tag{19}$$

where $n(\mathfrak{p}_1) = p^{f_1}, \cdots, n(\mathfrak{p}_r) = p^{f_r}$ and p has a similar decomposition in each of the conjugate fields. By a proof analogous to that given for the cubic equation,

$$\Delta_{\phi(p)} \equiv 0 \pmod{p}$$

where

$$\varphi(p) = p^{(e_1-1)f_1+(e_2-1)f_2+\cdots}(p^{f_1} - 1)(p^{f_2} - 1) \cdots.$$

If p is a divisor of Δ_q, and if it does not divide Δ_1 or the discriminant of (1), then q must be a divisor of $\varphi(p)$. Therefore q must either be equal to p (a case which we shall exclude presently) or otherwise, $kq + 1 = p^{f_1}$ and we thus have a tentative method of determining the factors of Δ_q similar to that given for quadratic and cubic equations.

The prime q can be equal to p only when it divides Δ_1, or in other words Δ_p cannot be divisible by p unless Δ_1 is divisible by p. This may be shown by proving that unless Δ_1 is divisible by p the number $\Delta_p \div \Delta_1$ is of the form $kp + 1$ and is therefore not a multiple of p. Thus for equation (1)

$$\Delta_p = 1 - \Sigma\alpha_i^p + \Sigma\alpha_i^p\alpha_j^p - \cdots.$$

We also have

$$(\Sigma\alpha_i)^p = (-a_1)^p, \qquad (\Sigma\alpha_i\alpha_j)^p = (a_2)^p, \qquad \text{etc.}$$

Hence expanding the left-hand members of these equations by the multinomial theorem and deleting integral multiples of p we obtain

$$\Sigma\alpha_i^p \equiv -a_1^p \equiv -a_1 \pmod{p}, \qquad \Sigma\alpha_i^p\alpha_j^p \equiv a_2^p \equiv a_2 \pmod{p}, \text{ etc.},$$

* Hilbert: l. c., p. 198; Bachmann: Allgemeine Arithmetik der Zahlenkoerper, p. 273.

therefore

$$\Delta_p \equiv 1 + a_1 + a_2 + \cdots + a_n \pmod{p}$$

or by § 2 we have $\Delta_p \equiv \Delta_1 \pmod{p}$. If now Δ_1 is not divisible by p then $\Delta_p/\Delta_1 \equiv 1 \pmod{p}$ or $\Delta_p/\Delta_1 = kp + 1$ as was to be proved.

If one of the prime ideals $\mathfrak{p}_i$ of (19) is of the first degree then one of the functions $P_i(x)$ of (18) is of the first degree and conversely. Under these conditions $f(x) \equiv 0 \pmod{p}$ has a real solution. We have

$$\begin{aligned} \alpha_1^{p-1} - 1 &\equiv 0 \pmod{\mathfrak{p}_i} \\ \alpha_2^{p-1} - 1 &\equiv 0 \pmod{\mathfrak{p}_i'} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{aligned}$$

where $\mathfrak{p}_i'$, $\mathfrak{p}_i''$, $\cdots$ are prime ideals conjugate to $\mathfrak{p}_i$. Then $\Pi(1 - \alpha_i^{p-1}) = \Delta_{p-1}$ must be a number of the ideal

$$\mathfrak{p}_i\mathfrak{p}_i'\mathfrak{p}_i'' \cdots = n(\mathfrak{p}_i) = p$$

and hence

$$\Delta_{p-1} \equiv 0 \pmod{p}.$$

This is another proof that the condition for a real solution of $f(x) \equiv 0 \pmod{p}$ is that Δ_{p-1} be divisible by p.

8. **Characteristic Factors of Δ_m.** A very similar state of affairs exists for the divisors of Δ_m where m is composite, as for the divisors of Δ_q. For simplicity we shall confine ourselves to the cubic equation; the method of argument however is applicable to an equation of any degree.

Let us consider any prime factor p of Δ_m which is not a factor by virtue of being a factor of Δ_r where r divides m; such a factor we shall call a characteristic factor of Δ_m. The prime p will be of the first, second, or third class in the number fields generated by α_1, α_2, and α_3 and $\varphi(p)$ will be equal to $p - 1$, $p^2 - 1$, or $p^3 - 1$. Furthermore since p enters Δ_m as a factor and does not divide Δ_r where r divides m then α_1, α_2, and α_3 will belong to the exponent m. Thus m must divide $p - 1$, $p^2 - 1$, or $p^3 - 1$ and hence p, p^2, or p^3 is of the form $km + 1$.

Hence the characteristic factors p of Δ_m have the property that p, p^2, or p^3 is of the form $km + 1$.

A PROBLEM IN GEOMETRY CONNECTED WITH THE ANALYTIC CONTINUATION OF A POWER SERIES.*

By T. H. Gronwall.

Consider a power series $\sum_0^\infty c_n z^n$ convergent for $|z| < 1$, and such that the analytic function defined by it has the only singularity $z = -1$ at finite distance. At any point $z_0 \neq -1$ at finite distance, the function may then be expanded in powers of $z - z_0$, convergent for $|z - z_0| < |1 + z_0|$, and this power series is obtainable through analytic continuation of the original series successively to a number of points $a_1, a_2, \cdots, a_m, a_{m+1} = z_0$, each point lying within the circle of convergence of the power series belonging to the preceding point, so that

$$|a_1| < 1, \qquad |a_\nu - a_{\nu-1}| < |1 + a_{\nu-1}|, \qquad \nu = 1, 2, \cdots, m+1.$$

The question now arises: what is the *minimum* number m of intermediate points $a_1, a_2, \cdots, a_m$ necessary for the analytic continuation of the given power series to the point z_0?

It will be convenient to refer the points z to a polar coördinate system with the pole at $z = -1$ and the real axis as reference line, so that

$$z = -1 + re^{\theta i}, \qquad -\pi \leqq \theta \leqq \pi.$$

The set of points z_0 for which no intermediate points are necessary, or $m = 0$, evidently consists of the interior of the circle $|z| = 1$ or

$$r = 2\cos\theta, \qquad -\frac{\pi}{2} \leqq \theta \leqq \frac{\pi}{2}.$$

Generally, *the set of points z_0 for which no more than m intermediate points are necessary, consists of the interior of the curve*

$$(C_m) \qquad r = \left(2\cos\frac{\theta}{m+1}\right)^{m+1}, \qquad -\pi \leqq \theta \leqq \pi.\dagger$$

This statement being true for $m = 0$, we shall assume it proved for $C_0, C_1, \cdots, C_{m-1}$ and show its validity for C_m. Any point $z_0 = -1 + re^{\theta i}$ for which m or fewer intermediate points are necessary, must be interior to a circle passing through $z = -1$, with center at some point $z' =$

* Read before the American Mathematical Society, Sept. 2, 1916.

† For $m = 0$, we have instead $-(\pi/2) \leqq \theta \leqq (\pi/2)$.

$-1+r'e^{\theta' i}$ inside C_{m-1}, so that

$$r < 2r' \cos(\theta' - \theta), \qquad -\frac{\pi}{2} < \theta' - \theta < \frac{\pi}{2},$$

and since $r' < [2\cos(\theta'/m)]^m$, we obtain

$$f(\theta') = 2^{m+1}\left(\cos\frac{\theta'}{m}\right)^m \cos(\theta' - \theta) - r > 0, \tag{1}$$
$$-\frac{\pi}{2} < \theta' - \theta < \frac{\pi}{2}, \qquad -\pi \leqq \theta,\ \theta' \leqq \pi.$$

To obtain the upper bound of all r belonging to a given θ, we must evidently make $f(\theta')$ a maximum in respect to θ'; forming the derivative, we find the condition

$$f'(\theta') = 2^{m+1}\left(\cos\frac{\theta'}{m}\right)^{m-1} \sin\left(\theta - \frac{m+1}{m}\theta'\right) = 0. \tag{2}$$

The first factor does not vanish for $-\pi \leqq \theta' \leqq \pi$ (except for $m = 2$, $\theta' = \pm\pi$, which gives $f(\theta') < 0$), so that all solutions of (2) are given by

$$\theta' = \frac{m}{m+1}(\theta - k\pi), \qquad k \text{ integer.}$$

The condition $-(\pi/2) < \theta' - \theta < (\pi/2)$ becomes

$$-\frac{\pi}{2} - \frac{mk}{m+1}\pi < \frac{\theta}{m+1} < \frac{\pi}{2} - \frac{mk}{m+1}\pi,$$

and the condition $-\pi \leqq \theta' \leqq \pi$ gives

$$\frac{k\pi}{m+1} - \frac{\pi}{m} \leqq \frac{\theta}{m+1} \leqq \frac{k\pi}{m+1} + \frac{\pi}{m}.$$

Combining these two sets of inequalities, we find

$$-\frac{\pi}{2} - \frac{mk}{m+1}\pi < \frac{k\pi}{m+1} + \frac{\pi}{m}, \qquad \frac{k\pi}{m+1} - \frac{\pi}{m} < \frac{\pi}{2} - \frac{mk\pi}{m+1},$$

or

$$-\frac{1}{m} - \frac{1}{2} < k < \frac{1}{m} + \frac{1}{2},$$

whence $k = 0$.* Consequently

$$\theta' = \frac{m}{m+1}\theta, \tag{3}$$

and (1) gives $r < [2\cos(\theta/m+1)]^{m+1}$, which proves our proposition.

* Except possibly for $m = 1$. But then the condition $-\pi \leqq \theta' \leqq \pi$ is replaced by $-(\pi/2) \leqq \theta' \leqq (\pi/2)$, and we obtain $-(1/2m) - \frac{1}{2} < k < (1/2m) + \frac{1}{2}$, so that $k = 0$.

The above calculation is visibly identical with the one leading to the equation of the envelope of the circles $r = 2r' \cos(\theta' - \theta)$ passing through $z = -1$ and having their centers on the curve C_{m-1} or $r' = [2\cos(\theta'/m)]^m$. The curve C_m is not, however, the envelope of all these circles, since on account of $-\pi \leqq \theta \leqq \pi$, (3) confines θ' to the interval

$$-\frac{m\pi}{m+1} \leqq \theta' \leqq \frac{m\pi}{m+1}.\dagger$$

The circles belonging to values of θ' in the remainder of the interval $-\pi \leqq \theta' \leqq \pi$ evidently have as envelope the two arcs of the complete curve

$$r = \left(2\cos\frac{\theta}{m+1}\right)^{m+1}, \qquad -\frac{m+1}{m}\pi \leqq \theta \leqq -\pi \qquad \text{and}$$

$$\pi \leqq \theta \leqq \frac{m+1}{m}\pi.$$

The complete curve being symmetrical about the real axis, these two arcs are evidently also given by

$$(4)\qquad \begin{aligned} r &= \left(2\cos\frac{2\pi-\theta}{m+1}\right)^{m+1}, \qquad \frac{m-1}{m}\pi \leqq \theta \leqq \pi, \\ r &= \left(2\cos\frac{2\pi+\theta}{m+1}\right)^{m+1}, \qquad -\pi \leqq \theta \leqq -\frac{m-1}{m}\pi. \end{aligned}$$

By C_m' we shall denote the closed curve formed by these two arcs and the arc of circle given by

$$(5)\quad r = 2^{m+1}\left(\cos\frac{\pi}{m}\right)^m \cos(\pi - \theta), \qquad \frac{m-1}{m}\pi \leqq \theta \leqq \pi \qquad \text{and}$$

$$-\pi \leqq \theta \leqq -\frac{m-1}{m}\pi;$$

this circle evidently passes through $z = -1$ and has as center the double point $\theta = \pi$ of C_{m-1}.

The significance of C_m' for the analytic continuation will appear in the following problem: given a point $z_0 = -1 + re^{\theta i}$ inside C_m but out-

† If we consider the *complete* curve $r = (2\cos\theta/m + 1)^{m+1}$, i. e., let θ vary through all the values for which this equation gives $r \geqq 0$, it is readily seen that each of its points is obtained once when θ varies through the interval $-(m+1)\pi/2 < \theta \leqq (m+1)\pi/2$. The complete curve has double points at $\theta = k\pi$, $k = 1, 2, \cdots, \left[\frac{m+1}{2}\right]$ and consists of $\left[\frac{m+1}{2}\right] + 1$ loops, each interior to the preceding one. This curve is the special case $n = 1/(m+1)$ of the sine spiral $r^n = a^n \cos n\vartheta$, for the general properties of which compare H. Wieleitner, Spezielle ebene Kurven (Leipzig, 1908), pp. 131–142, and G. Loria, Spezielle algebraische und transcendente ebene Kurven, 2d ed., vol. 1 (Leipzig, 1908), pp. 470–482.

side or on C_{m-1}, so that the analytic continuation to z_0 requires at least m intermediate points $a_1, a_2, \cdots, a_m$; what are the possible positions of the last intermediate point a_m?

It is obvious that, since a_m is the center of a circle through $z = -1$ and containing z_0 in its interior, a_m and z_0 must lie on the same side of the perpendicular bisector of the segment joining z_0 to -1, and on the other hand, a_m must be interior to C_{m-1}.

We shall now see that for $m > 1$, *the possible positions of a_m thus defined form a single continuum, when z_0 is exterior to or on C_m', but two separate continua, when z_0 is interior to C_m'.* To prove this, it is evidently sufficient to show that the perpendicular bisector mentioned above intersects C_{m-1} in two and four points respectively. The equation of the perpendicular bisector in the coördinates r', θ' is

$$2r' \cos(\theta' - \theta) = r,$$

and hence the intersection points with C_{m-1} are given by

$$f(\theta') = 0, \qquad -\pi \leqq \theta' \leqq \pi,$$

where $f(\theta')$ is the function defined by (1). On account of the symmetry about the real axis, we may assume $0 \leqq \theta \leqq \pi$, and since $f(\theta') < 0$ unless $\cos(\theta' - \theta) > 0$, it follows from $-\pi \leqq \theta' \leqq \pi$ that any root of $f(\theta') = 0$ must lie in either of the intervals

$$-\frac{\pi}{2} < \theta' - \theta < \frac{\pi}{2} \qquad \text{or} \qquad -2\pi < \theta' - \theta < -\frac{3\pi}{2}.$$

Now let us examine the roots of $f'(\theta') = 0$ in these intervals. In the first, we have already found the only root (3); in the second we find, by substituting $\theta' = m(\theta - k\pi)/m + 1$ in the inequality defining the interval,

$$\frac{3\pi}{2} < \frac{\theta}{m+1} + \frac{mk}{m+1}\pi < 2\pi,$$

and combining this with $0 \leqq \theta \leqq \pi$, we obtain

$$\frac{3}{2} < \frac{mk+1}{m+1}, \qquad \frac{mk}{m+1} < 2,$$

whence $k = 2$ (and $m > 1$). Thus $f'(\theta') = 0$ has one root $\theta_1' = \dfrac{m(\theta - 2\pi)}{(m+1)}$ in the second, and another $\theta_2' = m\theta/(m+1)$ in the first of these intervals, and consequently either contains at most two roots of $f(\theta') = 0$. Now

$$f(\pm\pi) = -2^{m+1}\left(\cos\frac{\pi}{m}\right)^m \cos\theta - r,$$

$$
\begin{aligned}
f(\theta_1') &= 2^{m+1}\left(\cos\frac{2\pi-\theta}{m+1}\right)^{m+1} - r, \\
f(0) &= 2^{m+1}\cos\theta - r, \\
f(\theta_2') &= \left(2\cos\frac{\theta}{m+1}\right)^{m+1} - r,
\end{aligned} \tag{6}
$$

and since z_0 is inside C_m, we have $f(\theta_2') > 0$; observing furthermore that $f(-\pi) = f(\pi)$ and that $f(0) \geqq 0$ implies $f(\pm\pi) < 0$, we find the only possible sign combinations to be the following:

$f(-\pi)$	$f(\theta_1')$	$f(0)$	$f(\theta_2')$	$f(\pi)$
+	+	−	+	+
+	−	−	+	+
−	+	+	+	−
−	+	−	+	−
−	−	+	+	−
−	−	−	+	−

so that $f(\theta') = 0$ has either two or four roots, the latter being the case when $f(\pm\pi) < 0$, $f(\theta_1') > 0$, $f(0) < 0$. Here $f(\pm\pi) < 0$ signifies that z_0 is outside the circle (5). The conditions $\theta \leqq \pi$ and $-\pi \leqq \theta_1'$ give $(m-1)\pi/m \leqq \theta \leqq \pi$, and consequently $f(\theta_1') > 0$ signifies that z_0 lies between the upper of the two arcs defined by (4) and the real axis. Hence z_0 is inside C_m', and since $\theta \geqq \pi/2$, we have also $f(0) < 0$, so that all the conditions for four roots are satisfied.

ON THE POWER SERIES FOR LOG $(1 + z)$.*

By T. H. Gronwall.

Let z and ζ be complex variables, define e^ζ by the power series

$$e^\zeta = \sum_{n=0}^{\infty} \frac{\zeta^n}{n!}, \tag{1}$$

and write $1 + z = e^\zeta$, or

$$z = \zeta + \frac{\zeta^2}{2!} + \cdots + \frac{\zeta^n}{n!} + \cdots.$$

By the inversion theorem for power series, there exists a unique power series in z without constant term, convergent for $|z|$ sufficiently small, and which substituted for ζ reduces the above relation to an identity. This series we now take as the definition of $\log (1 + z)$; its coefficients are most readily calculated by observing that $d\zeta/dz = e^{-\zeta} = 1/(1 + z)$, and we find

$$\log (1 + z) = \zeta = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} z^n, \quad \text{convergent for } |z| < 1. \tag{2}$$

The following two fundamental properties of the logarithm may be proved in various ways:

I. The analytic function $\log (1 + z)$ defined by (2) has $z = -1$ as its only singular point at finite distance.

II. The analytic continuation of $\log (1 + z)$ along a closed path winding once in the positive sense about $z = -1$ increases that function by $2\pi i$.

It is the purpose of the present note to establish these properties by actually performing the analytic continuation of the power series (2), and the proofs employed are sufficiently simple to serve as illustrations of the process of analytic continuation in an introductory course on the theory of functions of a complex variable.

It is well known that when the power series $\sum_{n=0}^{\infty} c_n(z - a)^n$, convergent for $|z - a| < r$, is continued analytically to the point a', where $|a' - a| < r$, the result is

$$\sum_{n=0}^{\infty} c_n(z - a)^n = \sum_{n=0}^{\infty} c_n'(z - a')^n, \tag{3}$$

where

$$c_n' = \sum_{\nu=0}^{\infty} \frac{(n + \nu)!}{n!\,\nu!} c_{n+\nu}(a' - a)^\nu, \tag{4}$$

* Read before the American Mathematical Society, Sept. 2, 1916.

and the identity (3) is valid at least for $|z - a'| < r - |a' - a|$, the latter expression being also a lower bound for the radius of convergence of the series to the right in (3). For $a = 0$, $a' = a_1$, where $|a_1| < 1$, and $c_n = (-1)^{n-1}/n$, formula (4) gives

$$c_n' = \sum_{\nu=0}^{\infty} \frac{(n+\nu)!}{n!\,\nu!} \frac{(-1)^{n+\nu-1} a_1^{\nu}}{n+\nu} = \frac{(-1)^{n-1}}{n} \sum_{\nu=0}^{\infty} \frac{(n+\nu-1)!}{(n-1)!\,\nu!} (-a_1)^{\nu}$$

$$= \frac{(-1)^{n-1}}{n} \cdot \frac{1}{(1+a_1)^n}, \qquad (n \geqq 1),$$

the last result being obtained by making $z = -a_1$ in the expansion

$$\frac{1}{(1-z)^n} = \sum_{\nu=0}^{\infty} \frac{(n+\nu-1)!}{(n-1)!\nu!} z^{\nu}, \qquad (n \geqq 1 \text{ and } |z| < 1),$$

which is immediately verified by multiplying $n - 1$ times by itself the identity

$$\frac{1}{1-z} = \sum_{\nu=0}^{\infty} z^{\nu},$$

or differentiating it $n - 1$ times. Thus the analytic continuation of (2) to the point a_1, where $|a_1| < 1$, gives the power series

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} a_1^n + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n(1+a_1)^n} (z - a_1)^n$$

and its radius of convergence is seen at once, for instance by the ratio test, to be $|1 + a_1|$.

The analytic continuation to the point a_2, where $|a_2 - a_1| < |1 + a_1|$, has as coefficient of $(z - a_2)^n$ the expression

$$\sum_{\nu=0}^{\infty} \frac{(n+\nu)!}{n!\,\nu!} \frac{(-1)^{n+\nu-1}}{n+\nu} \frac{(a_2 - a_1)^{\nu}}{(1+a_1)^{n+\nu}} = \frac{(-1)^{n-1}}{n(1+a_1)^n} \cdot \frac{1}{\left(1 + \dfrac{a_2 - a_1}{1 + a_1}\right)^n}$$

$$= \frac{(-1)^{n-1}}{n} \cdot \frac{1}{(1+a_2)^n} \quad \text{for} \quad n \geqq 1,$$

so that we next obtain the power series

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} a_1^n + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \left(\frac{a_2 - a_1}{1 + a_1}\right)^n + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n(1+a_2)^n} (z - a_2)^n,$$

with a radius of convergence equal to $|1 + a_2|$.

Proceeding thus by successive analytic continuation to the points $a_1, a_2, \cdots, a_m$, where

(5) $\qquad |a_1| < 1, \qquad |a_\nu - a_{\nu-1}| < |1 + a_{\nu-1}|, \qquad \nu = 2, 3, \cdots, m,$

we obtain the power series

$$(6)\quad \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\left[a_1{}^n+\left(\frac{a_2-a_1}{1+a_1}\right)^n+\left(\frac{a_3-a_2}{1+a_2}\right)^n+\cdots+\left(\frac{a_m-a_{m-1}}{1+a_{m-1}}\right)^n\right]+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n(1+a_m)^n}(z-a_m)^n,$$

with a radius of convergence equal to $|1+a_m|$. Thus the circle of convergence of each of the analytic continuations (6) passes through the point $z=-1$. Now let z_0 be any point at finite distance distinct from -1; then we may join the origin to z_0 by a path not passing through -1 (for instance, the straight line from 0 to z_0, unless z_0 lies on the negative real axis, in which case we may use the straight line from 0 to $\frac{1}{2}i$ and the straight line from $\frac{1}{2}i$ to z_0). Let l be the length of this path, $d>0$ the minimum distance of any of its points from $z=-1$, and m an integer greater than l/d; then dividing the length of the path into m equal parts, denoting the division points by $a_1, a_2, \cdots, a_{m-1}$ and making $a_m=z_0$, we evidently have a sequence of points satisfying (5), so that the power series (2) may be continued analytically to the point $z_0(\neq -1)$. The only singular point at finite distance is therefore $z=-1$.

To establish property II, we observe that the analytic continuations of (2) along two paths, both of which begin and end at the origin, and wind once in the positive sense about $z=-1$, yield the same result. We may therefore use the path $a_0a_1a_2\cdots a_m$, where

$$a_\nu=-1+e^{2\nu\pi i/m},\qquad \nu=0,1,\cdots,m,$$

so that $a_0=a_m=0$. Here π is of course defined as the smallest positive root of $e^{2\pi i}=1$. We find that (5) is satisfied when

$$\left|\frac{a_\nu-a_{\nu-1}}{1+a_{\nu-1}}\right|=|e^{2\pi i/m}-1|<1,$$

which is certainly the case for m sufficiently large, since $e^{2\pi i/m}-1\to 0$ as $m\to\infty$ by (1). From (6) and (2) it follows, on account of $a_0=a_m=0$, that the analytic continuation increases (2) by the constant

$$K=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\sum_{\nu=1}^{m}\left(\frac{a_\nu-a_{\nu-1}}{1+a_{\nu-1}}\right)^n,$$

or substituting the values of a_ν,

$$K=m\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}(e^{2\pi i/m}-1)^n.$$

But by the remark made above regarding equivalent paths, the value of

K is independent of m, and may therefore be evaluated by letting m tend to infinity. From (1) we find

$$m(e^{2\pi i/m} - 1) \to 2\pi i \qquad \text{as} \qquad m \to \infty,$$

so that

$$|e^{2\pi i/m} - 1| < \frac{A}{m},$$

where A is a constant independent of m. Hence for $m > A$,

$$\left| m \sum_{n=2}^{\infty} \frac{(-1)^{n-1}}{n} (e^{2\pi i/m} - 1)^n \right| < m \sum_{n=2}^{\infty} \left(\frac{A}{m}\right)^n = \frac{A^2}{m - A} \to 0 \qquad \text{as} \qquad m \to \infty,$$

and substituting these results in the expression for K, we finally obtain

$$K = 2\pi i.$$

ON THE CONVERGENCE OF BINET'S FACTORIAL SERIES FOR LOG $\Gamma(s)$ AND $\psi(s)$.*

By T. H. Gronwall.

It is the purpose of the present note to extend to the boundary of the region of convergence the discussion of the series in question given in § 14 of Jensen's "An elementary exposition of the theory of the gamma function."†

Writing (J 13, 14 and J 27, 28)

$$\omega(s) = \log \Gamma(s) - (s - \tfrac{1}{2}) \log s + s - \log \sqrt{2\pi}$$
$$= \sum_0^\infty \left[(s + \nu + \tfrac{1}{2}) \log \frac{s + \nu + 1}{s + \nu} - 1 \right],$$
$$\omega^*(s) = \log s - \psi(s)$$
$$= \sum_0^\infty \left[\frac{1}{s + \nu} - \log \left(1 + \frac{1}{s + \nu} \right) \right],$$

the four Binet series are (J 53, 54, 55, 56)

$$(1) \qquad \omega(s) = \sum_1^\infty \frac{k_n}{n(s)_n}, \qquad k_n = \int_{-1}^0 (t + \tfrac{1}{2})(t)_n dt;$$

$$(2) \qquad \omega(s) = \sum_1^\infty \frac{k_n}{n(s + 1)_n}, \qquad k_n = \int_0^1 (t - \tfrac{1}{2})(t)_n dt;$$

$$(3) \qquad \omega^*(s) = \sum_1^\infty \frac{k_n}{n(s)_n}, \qquad k_n = -\int_{-1}^0 (t)_n dt;$$

$$(4) \qquad \omega^*(s) = \sum_1^\infty \frac{k_n}{n(s + 1)_n}, \qquad k_n = \int_0^1 (t)_n dt;$$

where

$$(5) \qquad (s)_n = s(s + 1) \cdots (s + n - 1) = \frac{\Gamma(s + n)}{\Gamma(s)}.$$

It is shown in J § 14 that all four Binet series are *absolutely* and *uniformly* convergent for $\Re(s) \geqq \epsilon > 0$, but divergent for $\Re(s) < 0$, where ϵ is arbitrarily small.

---

* Read before the American Mathematical Society, Sept. 2, 1916.

† Authorized translation, with additional notes, by T. H. Gronwall, these *Annals*, ser. 2, vol. 17 (1916), pp. 124–166. References to formulas in this paper will be given thus: (J53).

I now propose to show that

The series (1) *to* (4) *are all* UNIFORMLY, *and* (1) *and* (3) ABSOLUTELY *convergent for* $|s| \geqq \epsilon$, $\Re(s) \geqq 0$, *where* ϵ *is arbitrarily small, but* (2) *and* (4) *are not* ABSOLUTELY *convergent for* $\Re(s) = 0$.

The proof will consist in obtaining comparison series by means of asymptotic expressions for the various coefficients k_n.

From the first part of (5) and Euler's product for $\Gamma(s)$ (J 3) it is seen at once that

$$(t)_n = \frac{(n-1)!\,n^t}{\Gamma(t)} \cdot \prod_{\nu=n}^{\infty} \frac{\left(1+\frac{1}{\nu}\right)^t}{1+\frac{t}{\nu}},$$

and from the expansion

$$t\log\left(1+\frac{1}{\nu}\right) - \log\left(1+\frac{t}{\nu}\right) = \frac{t}{\nu} - \frac{t}{2\nu^2} + \frac{t}{3\nu^3} - \cdots + (-1)^{\mu+1}\frac{t}{\mu\nu^\mu} + \cdots - \left[\frac{t}{\nu} - \frac{t^2}{2\nu^2} + \frac{t^3}{3\nu^3} - \cdots + (-1)^{\mu+1}\frac{t^\mu}{\mu\nu^\mu} + \cdots\right]$$

it follows that for $-1 \leqq t \leqq 1$

$$\left| t\log\left(1+\frac{1}{\nu}\right) - \log\left(1+\frac{t}{\nu}\right) \right| \leqq \frac{1}{\nu^2} + \frac{1}{\nu^3} + \frac{1}{\nu^4} + \cdots = \frac{1}{\nu(\nu-1)},$$

$$\left| \sum_{\nu=n}^{\infty} \left[t\log\left(1+\frac{1}{\nu}\right) - \log\left(1+\frac{t}{\nu}\right)\right] \right| \leqq \sum_{\nu=n}^{\infty} \frac{1}{\nu(\nu-1)} = \frac{1}{n-1} < \frac{2}{n} \quad \text{for } n > 2,$$

$$\left| \prod_{\nu=n}^{\infty} \frac{\left(1+\frac{1}{\nu}\right)^t}{1+\frac{t}{\nu}} - 1 \right| < |e^{2/n} - 1| < \frac{c_1}{n},$$

where c_1 is some constant independent of n, so that finally

$$(t)_n = \frac{(n-1)!\,n^t}{\Gamma(t)}\left(1 + O\left(\frac{1}{n}\right)\right).* \tag{6}$$

Now, by (6), (1) and (3) have a k_n of the form

$$k_n = (n-1)! \int_{-1}^{0} F(t)[n^t + O(n^{t-1})]dt,$$

* The notation $f(x) = O(g(x))$, now quite commonly used in asymptotic calculations, signifies that there exist an $A > 0$ and an x_0 sufficiently large such that $|f(x)| < Ag(x)$ for $x > x_0$. It is evident from this definition that if $f_1(x) = O(g_1(x))$ and $f_2(x) = O(g_2(x))$, then $f_1(x)f_2(x) = O(g_1(x)g_2(x))$, and $f_1(x) + f_2(x) = O(g_1(x))$ if $g_1(x) \geqq g_2(x)$ for $x > x_0$.

where $F(t) = (t + \frac{1}{2})/\Gamma(t)$ or $-1/\Gamma(t)$ is holomorphic in the interval of integration and vanishes at both its ends; hence, integrating twice by parts

$$\int_{-1}^{0} F(t)n^t dt = \left[-\frac{F'(t)n^t}{(\log n)^2} \right]_{-1}^{0} + \frac{1}{(\log n)^2} \int_{-1}^{0} F''(t)n^t dt,$$

and by the first theorem of the mean

$$\left| \int_{-1}^{0} F''(t)n^t dt \right| < \int_{-1}^{0} |F''(t)| dt,$$

so that

$$\int_{-1}^{0} F(t)n^t dt = O\left(\frac{1}{(\log n)^2} \right).$$

By a further application of the first theorem of the mean

$$\int_{-1}^{0} F(t)O(n^{t-1})dt = O\left(\frac{1}{n} \right),$$

so that finally

$$k_n = O\left(\frac{(n-1)!}{(\log n)^2} \right).$$

Consequently, the series (1) and (3) are absolutely and uniformly convergent whenever this is the case with the series

$$\sum_{2}^{\infty} \left| \frac{(n-1)!}{n(\log n)^2 (s)_n} \right|.$$

But for $s = x + iy$, $x \geqq 0$ and $\nu > 0$, we have $|s + \nu|^2 = (\nu + x)^2 + y^2 \geqq \nu^2$, whence by (5)

$$|(s)_n| \geqq |s| \cdot 1 \cdot 2 \cdots (n-1), \tag{7}$$

so that, for $x = \Re(s) \geqq 0$ and $|s| \geqq \epsilon$,

$$\sum_{2}^{\infty} \left| \frac{(n-1)!}{n(\log n)^2 (s)_n} \right| \leqq \frac{1}{\epsilon} \sum_{2}^{\infty} \frac{1}{n(\log n)^2},$$

and the latter series being convergent, the first half of our proposition follows.

In the series (2) and (4), we have, by (6), a k_n of the form

$$k_n = (n-1)! \int_0^1 F(t)[n^t + O(n^{t-1})]dt,$$

where $F(t)$ is holomorphic in the integration interval and $F(0) = 0$, but $F(1) \neq 0$. Treating this integral in the same manner as before, we find

$$k_n = \frac{n!\,F(1)}{\log n} + O\left(\frac{n!}{(\log n)^2} \right).$$

The same argument as before shows that the series arising from the second term of k_n in (2) and (4) is absolutely and uniformly convergent for $\Re(s) \geqq 0$, so that now our comparison series becomes

$$\sum_{2}^{\infty} \frac{(n-1)!}{\log n \cdot (s+1)_n}. \tag{8}$$

To this series, we shall apply Dirichlet's convergence test.* We begin by showing that

$$A_n(s) = \sum_{\nu=1}^{n} \frac{(\nu-1)!}{(s+1)_\nu}$$

is uniformly bounded for $|s| \geqq \epsilon$, $\Re(s) \geqq 0$. From (5) we obtain the identity

$$\frac{(\nu-1)!}{(s+1)_{\nu-1}} - \frac{\nu!}{(s+1)_\nu} = \frac{(\nu-1)!}{(s+1)_{\nu-1}}\left(1 - \frac{\nu}{s+\nu}\right) = s \cdot \frac{(\nu-1)!}{(s+1)_\nu},$$

and making $\nu = 1, 2, \cdots, n$ and adding

$$A_n(s) = \frac{1}{s}\left(1 - \frac{n!}{(s+1)_n}\right).$$

For $\Re(s) \geqq 0$, we have, in analogy to (7), $|(s+1)_n| \geqq n!$, and consequently

$$|A_n(s)| \leqq \frac{1}{|s|}(1+1) \leqq \frac{2}{\epsilon} \quad \text{for} \quad |s| \geqq \epsilon \quad \text{and} \quad \Re(s) \geqq 0.$$

From the identity

$$\sum_{\nu=n}^{n+p} \frac{(\nu-1)!}{\log \nu (s+1)_\nu} = \sum_{\nu=n}^{n+p} \frac{A_\nu(s) - A_{\nu-1}(s)}{\log \nu}$$

$$= \sum_{\nu=n}^{n+p-1} A_\nu(s)\left(\frac{1}{\log \nu} - \frac{1}{\log(\nu+1)}\right) + \frac{A_{n+p}(s)}{\log(n+p)} - \frac{A_{n-1}(s)}{\log n}$$

we now obtain, since $1/\log \nu$ decreases as ν increases,

$$\left|\sum_{\nu=n}^{n+p} \frac{(\nu-1)!}{\log \nu (s+1)_\nu}\right| \leqq \frac{2}{\epsilon}\sum_{\nu=n}^{n+p-1}\left(\frac{1}{\log \nu} - \frac{1}{\log(\nu+1)}\right) + \frac{2}{\epsilon}\cdot\frac{1}{\log(n+p)} + \frac{2}{\epsilon}\cdot\frac{1}{\log n}$$

$$= \frac{4}{\epsilon}\cdot\frac{1}{\log n},$$

and the last expression is independent of s and may be made as small as we please by taking n sufficiently large. Thus (2) and (4) are uniformly convergent when $|s| \geqq \epsilon$, $\Re(s) \geqq 0$. Regarding the absolute convergence of (8) we observe that, since $\Gamma(s) = \lim_{n\to\infty} (n-1)!n^s/(s)_n$, we have for a

* Journ. de Math., ser. 2, vol. 7, pp. 253–255.

fixed s and an n sufficiently large

$$\frac{1}{2}\left|\frac{\Gamma(s+1)}{n^{s+1}}\right| < \left|\frac{(n-1)!}{(s+1)_n}\right| < 2 \cdot \left|\frac{\Gamma(s+1)}{n^{s+1}}\right|,$$

so that the series of absolute values in (8) will converge or diverge with

$$\sum_2^\infty \frac{1}{\log n \,|\, n^{s+1} \,|} = \sum_2^\infty \frac{1}{n^{1+\Re(s)} \cdot \log n}.$$

Hence (8) is absolutely convergent when $\Re(s) > 0$, but not when $\Re(s) = 0$.

NOTE ON CAUCHY'S INTEGRAL FORMULA.

By J. L. Walsh.

It is the object of this note to establish Cauchy's Integral Formula by means of the theorem* which is usually called " the mean value theorem for harmonic functions," but which can also be called the " mean value theorem for conjugate functions." Two functions $u(x, y)$ and $v(x, y)$ are said to be conjugate in a region T of the x, y-plane if throughout this region they are single-valued, continuous, and have continuous first partial derivatives, and also

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}. \tag{1}$$

If u and v are conjugate functions in a simply connected region T, it is shown below without assuming the existence of second derivatives† that

$$\frac{1}{2\pi r}\int u(x, y)ds = u(x_0, y_0), \tag{2}$$

$$\frac{1}{2\pi r}\int v(x, y)ds = v(x_0, y_0), \tag{3}$$

where the integrals are extended around any circle lying wholly within T, the radius of the circle being denoted by r and the center by (x_0, y_0).

Suppose that, within T, $f(z) = u(x, y) + iv(x, y)$ is an analytic and single-valued function of z, where $z = x + iy$. Then u and v are conjugate functions throughout T, so that equations (2) and (3) are true, the integrals being taken around the circle described above. Multiplying (3) by i and adding it to (2), we have

$$\frac{1}{2\pi r}\int f(z)ds = f(z_0), \qquad z_0 = x_0 + iy_0. \tag{4}$$

If z is on the circle, the use of polar coördinates gives

$$z - z_0 = r(\cos\varphi + i\sin\varphi),$$

* This is the reverse of the procedure common in books on Theory of Functions. For example, in Burkhardt, Funktionentheorie, § 36, the mean value theorem for harmonic functions is derived from Cauchy's Integral Formula by the use of essentially the same analytic machinery as that employed here.

† It is, of course, true that u and v have continuous second partial derivatives; but we must not assume that fact at this point if we wish to prove it later by means of Cauchy's integral formula, as is commonly done.

$$dz = r(-\sin\varphi + i\cos\varphi)d\varphi,$$
$$= \frac{i(z - z_0)}{r}ds.$$

Substituting the value of ds in (4), we have

$$\frac{1}{2\pi i}\int \frac{f(z)}{z - z_0}dz = f(z_0),$$

where the integral is taken around a circle whose center is z_0. As the formula is true for this particular path surrounding z_0, it is true, by Cauchy's theorem, for any path within T surrounding z_0 once in the positive direction.

The proof* of formulas (2) and (3) is as follows. Using polar coördinates (ρ, φ) with the pole at (x_0, y_0),

$$\frac{\partial u}{\partial \rho} = \frac{\partial u}{\partial x}\cos\varphi + \frac{\partial u}{\partial y}\sin\varphi,$$
$$\frac{1}{\rho}\frac{\partial v}{\partial \varphi} = \frac{\partial v}{\partial x}\cos\left(\varphi + \frac{\pi}{2}\right) + \frac{\partial v}{\partial y}\sin\left(\varphi + \frac{\pi}{2}\right)$$
$$= \frac{\partial u}{\partial \rho}$$

by equations (1). Then

$$\int_0^{2\pi}\frac{\partial u}{\partial \rho}d\varphi = \frac{1}{\rho}\int\frac{\partial u}{\partial \rho}ds = \frac{1}{\rho}\int\frac{1}{\rho}\frac{\partial v}{\partial \varphi}ds = \frac{1}{\rho}\int\frac{\partial v}{\partial s}ds = 0,$$

all the integrals being taken around a circle whose radius is ρ and center (x_0, y_0). Hence

$$0 = \int_0^r d\rho\int_0^{2\pi}\frac{\partial u}{\partial \rho}d\varphi = \int_0^{2\pi}d\varphi\int_0^r\frac{\partial u}{\partial \rho}d\rho = \int_0^{2\pi}[u(x, y) - u(x_0, y_0)]d\varphi;$$

$$\therefore\quad u(x_0, y_0) = \frac{1}{2\pi}\int_0^{2\pi}u(x, y)d\varphi$$
$$= \frac{1}{2\pi r}\int u(x, y)ds.$$

Similarly

$$v(x_0, y_0) = \frac{1}{2\pi r}\int v(x, y)ds,$$

the integrals being taken around a circle lying wholly within T, the radius of the circle being r and the center (x_0, y_0).

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.,
April, 1916.

* This proof is the proof given by M. Bôcher, "Gauss's Third Proof of the Fundamental Theorem of Algebra," Bull. Amer. Math. Society, vol. I (Second Series) (1894–95), pages 206, 207.

ON THE RATIONAL, INTEGRAL INVARIANTS OF NILPOTENT ALGEBRAS.*

By Olive C. Hazlett.

Introduction.

§ 1. Relation to literature. In the study of linear algebras, their invariantive classification is one of the most important problems. Peirce, Study, Scheffers, Hawkes, and others* have classified, over the field C of ordinary complex numbers, linear associative algebras in a small number of units; and associative algebras having less than four units, with a modulus, are easily characterized invariantively by invariants obtainable from the characteristic determinants,† but such invariants are not sufficient for the characterization of quaternary associative algebras with a modulus.‡ In view of Wedderburn's§ generalization of a theorem of Cartan,‖ we can go a long way toward characterizing the general linear algebra if we can characterize three special kinds of algebras; namely, matric algebras, division algebras, and nilpotent algebras. Over the field C, there is only a finite number of classes of the first two kinds of algebras of a given order; whereas, over the field C, there is an infinite number of classes of nilpotent algebras of any order greater than two; and hence, we centre our attention on nilpotent algebras.

In this paper, we consider rational, integral invariants of such algebras. Now all invariants obtainable from the characteristic determinants are zero for nilpotent algebras; and furthermore, there are no rational, integral invariants (other than constants) for n-ary nilpotent algebras under the total n-ary linear group. We accordingly consider invariants under the group which leaves unaltered the canonical form. For such rational, integral invariants this paper proves theorems analogous to theorems about invariants of algebraic forms, and in particular proves their finiteness. The fundamental invariants are found for the simpler cases.

* Written while the author was Alice Freeman Palmer Fellow of Wellesley College, 1915–16.

* B. Peirce, American Journal of Mathematics, vol. 4, p. 97; Study, Goettinger Nachrichten, 1889, p. 237; G. Scheffers, Mathematische Annalen, vol. 39, p. 293; Hawkes, American Journal of Mathematics, vol. 24, p. 87, Transactions, vol. 3, p. 312; Cayley, Collected Papers, pp. 60, 105; Buchheim, Messenger of Mathematics, series 2, vol. 16, p. 62.

† Hazlett, Annals of Mathematics, series 2, vol. 16, p. 1.

‡ Hazlett, Chicago Dissertation, § 1, American Journal of Mathematics, vol. 38.

§ Proceedings of London Math. Society, series 2, vol. 6, p. 109.

‖ Annales de Toulouse, séries 1, vol. 12, *B*.

§ 2. **Definitions.** A *linear algebra** over the field F is a set of hypercomplex numbers of the form $X = \sum_{i}^{1..n} x_i e_i$ where the *coördinates* x_i range independently over F, and where the *units* e_i are such that

$$e_i e_j = \sum_{k}^{1..n} \gamma_{ijk} e_k \qquad (i, j = 1, \cdots, n),$$

where (i) the *constants of multiplication* γ_{ijk} are in F, (ii) the sum of two numbers X and Y of the algebra is $X + Y = \sum_{i}^{1..n} (x_i + y_i) e_i$ and (iii) numbers of the algebra combine under addition and multiplication according to the distributive law. Unless explicitly stated, we do not assume the commutative nor the associative law of multiplication. A linear algebra A which is such that, for some integer α, $A^\alpha = 0$, is said to be nilpotent.† If α is the smallest such number, α is called the *index* of the algebra.

The *complex*‡ $C = (x_1, \cdots, x_a)$ is defined as the set of all quantities linearly dependent on $x_1, \cdots, x_a$; and the number of linearly independent elements of the complex is called its *order*. If C_1 and C_2 are two complexes, the complex formed by all quantities linearly dependent on the elements of C_1 and C_2 is called the *sum* of C_1 and C_2 and is denoted by $C_1 + C_2$. If y_1 and y_2 are any elements of C_1 and C_2 respectively, the complex of all elements linearly dependent on those of the form $y_1 y_2$ is called the *product* of C_1 by C_2 and is written $C_1 C_2$. If a complex C_2 is contained in a complex C_1, we write $C_2 \leq C_1$.

Suppose we have given the n-ary algebra $A = (e_1, \cdots, e_n)$ with the constants of multiplication γ_{ijk} and the n-ary algebra $A' = (e_1', \cdots, e_n')$ with constants of multiplication γ_{ijk}'. If there exist a non-singular linear homogeneous transformation of the group L on the units of A such that, for the transformed algebra A', the constants of multiplication are equal to the corresponding γ_{ijk}', then A and A' are said to be *equivalent* with respect to the group L. The totality of all algebras equivalent with respect to a group L are said to constitute a *class* of algebras with respect to that group.

Now we know§ that, if A be a nilpotent algebra (not necessarily associative) with index α, then A is the sum of $\alpha - 1$ non-overlapping complexes $B_1, \cdots, B_{a-1}$, such that

$$B_p B_q \leq \sum_{r=p+q}^{a-1} B_r.$$

* For other definitions, see Dickson, Transactions, vol. 4, p. 26.

† For a statement of the two essentially different definitions of a nilpotent algebra see author's dissertation or Wedderburn, l. c., p. 87. The one used here is that due to Wedderburn.

‡ Wedderburn, l. c., p. 79.

§ Wedderburn, l. c., p. 87.

In fact $B_i \equiv A^i \pmod{A^{i+1}}$ for every i. The orders of the complexes B_i are invariants, though the complexes themselves are not invariantive. Moreover, any algebra which can be put in this form is necessarily nilpotent. Hence if a nilpotent algebra be in the above form and such that $B_1 = (e_1, \cdots, e_{\nu'})$ and in general $B_i = (e_{\nu^{(i-1)}+1}, \cdots, e_{\nu^{(i)}})$ $(i = 2, \cdots, \alpha - 1)$, then it is said to be in *canonical form.** Notice that $\nu^{(i)} = \sum_{j=1}^{i} n^{(j)}$ where $n^{(j)}$ is the order of B_j. If $n^{(i)}$ is the order of B_i $(i = 1, \cdots, \alpha - 1)$, the nilpotent algebra of index α is said to be of *genus* $(\alpha; n', \cdots, n^{(\alpha-1)})$.

Invariants for the general nilpotent algebra.

§ 3. Rational, integral invariants of n-ary nilpotent algebra under total n-ary linear group. Consider those rational, integral functions of the constants of multiplication of the general n-ary linear algebra which are invariant under the total linear group of transformations on the n units. Any such invariant I has certain properties analogous to the isobarism of the rational, integral invariants for algebraic forms.

To show this, we need the notion of "weight." Now if we have the algebra

$$e_i e_j = \sum_{k}^{1..n} \gamma_{ijk} e_k \qquad (i, j = 1, \cdots, n),$$

then, when we multiply e_r by $\lambda \neq 0$, and leave other units unchanged, the γ's are subject to the induced transformation where γ_{ijk} is unaltered when $i, j, k \neq r$, and where γ_{ijr} $(i, j \neq r)$ is multiplied by λ^{-1}, γ_{rir} and γ_{irr} $(i \neq r)$ by λ^0, γ_{rrr} by λ, γ_{rjk} and γ_{jrk} $(j, k \neq r)$ by λ and γ_{rrk} $(k \neq r)$ by λ^2. Hence, for convenience, we say that γ_{ijk} $(i, j, k \neq r)$ is of weight 0 in e_r, γ_{ijr} $(i, j \neq r)$ of weight -1 in e_r, γ_{rir} and γ_{irr} $(i \neq r)$ of weight 0, γ_{rrr} of weight 1, γ_{rjk} and γ_{jrk} $(j, k \neq r)$ of weight 1, and γ_{rrk} $(k \neq r)$ of weight 2 in e_r. And we do this for every r. For every unit e_r, we thus assign to γ_{ijk} a weight with respect to that unit, which is counted up in the following way: the first subscript, i, contributes $+1$ toward this weight if $i = r$, but 0 if $i \neq r$; the second, j, contributes $+1$ if $j = r$, otherwise 0; and the third, k, contributes -1 if $k = r$, otherwise 0. The sum of these three partial weights is called the *weight of γ_{ijk} with respect to e_r.*

If we consider a particular rational, integral invariant I of the kind described above, then I is isobaric in e_1. For, if we multiply e_1 by a scalar $\lambda \neq 0$, then the γ's are multiplied as follows,—γ_{111} is multiplied by λ, the γ_{11i} $(i \neq 1)$ are multiplied by λ^2, the γ_{1j1} and γ_{j11} $(j \neq 1)$ are multiplied by λ^0, the γ_{1jk} and γ_{j1k} $(j, k \neq 1)$ are multiplied by λ, the γ_{lm1} $(l, m \neq 1)$

* Author's dissertation, §§ 3, 5.

are multiplied by λ^{-1} and the remaining γ's are unaltered. But, since I is an invariant, we have

$$I(\gamma'_{ijk}) = F(\lambda)I(\gamma_{ijk})$$

where the γ'_{ijk} are the constants of multiplication for the transformed algebra. Hence our statement. In general we have

Lemma I. *For an n-ary linear algebra, a rational, integral invariant under the total n-ary linear group is isobaric in any particular unit e_i.*

Furthermore, since I must be invariant under the transformation which merely interchanges e_1 and e_l, the weight of I in e_1 must equal its weight in e_l, for every l. This is true only for invariants under the *total* linear group.

In particular, consider I when formed for a nilpotent algebra in canonical form. Some terms drop out, owing to the form of the multiplication table. The terms that remain (if any) cannot be of positive weight in e_n and cannot be of negative weight in e_1, and yet must be of the same weight in e_1 and e_n. Hence the terms that remain must be of weight zero in e_1 and e_n, and thus of weight zero in each unit. But for a nilpotent algebra in canonical form, each γ which is not zero is of positive or zero weight with respect to e_1, those of zero weight being the γ_{ijk} $(i, j, k \neq 1)$; and thus I here contains at most only the γ_{ijk} $(i, j, k \neq 1)$. Similarly I can not contain any γ's which depend on e_n. Then I can not contain any γ's which depend on any unit of B_1 or of B_{a-1}. Finally, by induction, I when formed for a nilpotent algebra in canonical form must be independent of all the γ's.

In this we have been considering rational, *integral* functions of the γ's, but the conclusion applies also to *any* rational function of the γ's. For consider the invariant $I = I_1/I_2$ where I_1 and I_2 are rational integral functions of the γ's with no common factor. Then, when we make a linear transformation on the units, the γ's are replaced by linear functions of the original γ's, and hence I_j $(j = 1, 2)$ is replaced by a rational integral function of the same degree as I_j. Thus, from the invariancy of I we infer that of I_1 and I_2. Accordingly we have

Theorem I. *Other than constants, there are no rational functions of the constants of multiplication which, under the total n-ary linear group, have the invariantive property for the general n-ary nilpotent algebra or even for a particular set of nilpotent algebras.* This is a generalization of the known fact that all invariants obtainable from the characteristic determinants reduce to zero for a nilpotent algebra.

Invariants for a nilpotent algebra in canonical form.

§ 4. Some properties of rational, integral invariants of nilpotent algebras of genus $(\alpha; n', \cdots, n^{(a-1)})$. In view of the theorem of the last section, we consider the general nilpotent algebra over the field F, of genus

$(\alpha;\ n',\ \cdots,\ n^{(\alpha-1)})$, in canonical form, and inquire into the properties of those rational, integral functions of the constants of multiplication of such an algebra which are invariant under the group G which leaves unaltered the canonical form. This group G consists of the totality of transformations of the form*

$$e_{i_p}' = \sum_{q=p}^{\alpha-1} \sum_{jq} a_{i_p j_q} e_{j_q}, \tag{1}$$

where e_{j_q} is a unit of B_q, e_{i_p}' a unit of B_p' and the a's are in F.

Lemma II. *A rational, integral invariant I of the general (n-ary) nilpotent algebra in canonical form under the group G is homogeneous in the constants of multiplication.* For, since I is invariant under the general transformation of G, it must in particular be invariant under the transformation $e_j' = \lambda e_j$ $(j = 1,\ \cdots,\ n)$ $(\lambda \neq 0)$.

Moreover, Lemma I holds for invariants under this group G. For convenience we shall accordingly borrow the term *gradient*, using it here to denote a homogeneous function of the constants of multiplication which is isobaric in each unit.

Although a rational, integral invariant I under G is isobaric in each unit, its weight in e_1 is not in general equal to its weight in e_j, since I is not in general invariant if we interchange e_1 and e_j. If, however, e_j is one of the units of B_1, then I must be invariant when we interchange e_1 and e_j; and thus we have

Lemma III. *For the general nilpotent algebra in canonical form, if I be of weight w_j in e_j, a unit of B_i, then it is of weight w_j in e_k where e_k is any unit of B_i.*

The invariancy of I is expressed by the formula

$$I(\gamma'_{ijk}) = \phi(a_{lm}) I(\gamma_{ijk}), \tag{2}$$

where the γ_{ijk} are the constants of multiplication of the original algebra, the a_{lm} are the coefficients of the transformation, and the γ'_{ijk} the constants of multiplication of the transformed algebra. Now we know from the theory of invariants for algebraic forms, that the factor by which a rational, integral invariant is multiplied under a linear transformation of the variables is a power of the determinant of the transformation, the exponent being given by a simple formula when we know the number of variables, and the degree and weight of our invariant. We would expect an analogous thing to happen here, and such is the case.

When we subject the units of the algebra $E = (e_1,\ \cdots,\ e_n)$ to the non-singular transformation

$$e_i' = \sum_{j}^{1,\,n} a_{ij} e_j \qquad (i = 1,\ \cdots,\ n),$$

* Author's dissertation, § 4.

then, if the γ_{ijk} be the constants of multiplication for E, and the γ'_{ijk} the constants of multiplication for the transformed algebra E',

$$\sum_p \gamma'_{ijp} a_{pq} = \sum_{k,l} a_{ik} a_{jl} \gamma_{klq} \qquad (i, j, q = 1, \cdots, n). \tag{3}$$

If in (3) we keep i and j fixed and let q range from 1 to n, we have n homogeneous equations in n unknowns γ'_{ijp} $(p = 1, \cdots, n)$ which we can solve uniquely.

Suppose that, in particular, we have a nilpotent algebra of genus $(\alpha; n', \cdots, n^{(\alpha-1)})$ in canonical form, and that we subject the units to the most general transformation of the group G which leaves unaltered units not in B_1. Then the units of B_1 are transformed according to

T_1:
$$e_{i_1}' = \sum_{\eta=1}^{\alpha-1} \sum_{j_\eta} a_{i_1 j_\eta} e_{j_\eta},$$

where the determinant

$$A_1 \equiv |a_{i_1 j_1}| \neq 0.$$

Then from (3) on account of the special form of the transformation we have

$$\gamma'_{i_1 j_1 p} = \sum_{k,l} a_{i_1 k} a_{j_1 l} \gamma_{klp},$$

$$\gamma'_{i_1 jp} = \sum_k a_{i_1 k} \gamma_{kjp} \qquad (j > n'),$$

$$\gamma'_{i_1 ip} = \sum_l a_{j_1 l} \gamma_{ilp} \qquad (i > n'),$$

while all other γ''s are equal to the corresponding γ's.

Now these formulæ show that, if I be a rational, integral invariant under G, of total weight $w^{(1)}$ in the units of B_1, then $I(\gamma'_{ijk})$ is a rational, integral homogeneous function of degree $w^{(1)}$ in the $a_{i_1 k}$. But $I(\gamma_{ijk})$ is independent of the coefficients of the transformation, and hence $\phi(a_{lm})$ for the transformation T, is a rational, integral homogeneous function ϕ_1 of degree $w^{(1)}$ in $a_{i_1 k}$. Thus

$$I(\gamma'_{ijk}) = \phi_1(a_{i_1 l}) I(\gamma_{ijk}).$$

Also

$$I(\gamma_{ijk}) = \phi_1(A_1^{-1} \cdot A_{li_1}) I(\gamma'_{ijk})$$
$$= A_1^{-w^{(1)}} \phi_1(A_{li_1}) I(\gamma'_{ijk}).$$

Combining these two results, we have

$$\phi_1(A_{ji_1}) \phi_1(a_{i_1 j}) = A_1^{w^{(1)}},$$

where both functions on the left are rational and integral in the $a_{i_1 j}$. But A_1 is an irreducible function of its elements, when these are regarded as independent variables, and hence

$$\phi_1(a_{i_1 j}) = k_1 A_1^{r_1}.$$

To find the value of r_1, we observe that $\phi_1(A_{ji_1})$ is of degree $r_1 n^{(1)}(n^{(1)} - 1)$ in the $a_{i_1 j}$, and hence

$$r_1 = \frac{w^{(1)}}{n^{(1)}}.$$

Furthermore $k_1 = 1$ as we can see by applying the identical transformation.

Similarly, if we subject the units to the most general transformation of the group G which leaves unaltered units not in B_2, the units of B_2 undergo the transformation

T_2:
$$e_{i_2}' = \sum_{q=2}^{a-1} \sum_{j_q} a_{i_2 j_q} e_{j_q},$$

where the determinant

$$A_2 \equiv |a_{i_2 j_2}| \neq 0.$$

Then

$$\gamma_{i_1 j_1 m_2} = \sum_{n_2} \gamma'_{i_1 j_1 n_2} a_{n_2 m_2},$$

$$\gamma_{i_1 j_1 m_p} = \sum_{n_2} \gamma'_{i_1 j_1 n_2} a_{n_2 m_p} + \gamma'_{i_1 j_1 m_p} \qquad (p > 2),$$

$$\gamma'_{i_2 j_2 m} = \sum_{k,l} a_{i_2 k} a_{j_2 l} \gamma_{klm},$$

$$\gamma'_{i_2 j_p m} = \sum_{k} a_{i_2 k} \gamma_{k j_p m} \qquad (p \neq 2),$$

$$\gamma'_{i_p j_2 m} = \sum_{l} a_{j_2 l} \gamma_{i_p l m} \qquad (p \neq 2),$$

while the other γ'_{ijk} are equal to the corresponding γ_{ijk}.

The proof for this case runs very much the same as for the first case, the differences being due to the facts that (i) the $\gamma'_{i_1 j_1 m_p}$ $(p > 2)$ are not in general homogeneous in the $a_{n_2 m}$ and hence conceivably $I(\gamma'_{ijk})$ may not be homogeneous in these a's; and (ii) $I(\gamma'_{ijk})$ is not in general integral in the $a_{n_2 m}$. The first difficulty is obviated when we observe that those terms in $a_{n_2 m}$ arising from the $\gamma_{i_1 j_1 m_p}$ $(p > 2)$ must cancel one another, inasmuch as these terms give rise to no terms of the requisite weight in the units of B_2. As for the second difficulty, we notice that the only way $I(\gamma'_{ijk}) \equiv I'(\gamma_{ijk})$ can fail to be integral in the $a_{n_2 m}$ is by having in the denominator A_2 raised to an integral power, thus:

$$I(\gamma'_{ijk}) \equiv I'(\gamma_{ijk}) \equiv \frac{1}{A_2^{\delta^{(2)}}} I''(\gamma_{ijk}),$$

where I'' is integral in the $a_{n_2 m}$, and therefore $A_2^{\delta^{(2)}} \phi_2(a_{i_2 j})$ is rational, integral and homogeneous in the $a_{i_2 j}$. Then, for this case we infer that

$$\phi_2(a_{i_2 j}) \equiv A_2^{\frac{w^{(2)}}{n^{(2)}}}.$$

We obtain a similar result for a transformation T_i which leaves unaltered the units of B_j $(j \neq i)$.

But the most general transformation T of the group G is the product of these transformations T_i, and thus we have

Theorem II. *For a nilpotent algebra* $E = \sum_{i=1}^{\alpha-1} B_i$ *of genus* $(\alpha; n', \cdots, n^{(\alpha-1)})$ *in canonical form, let* $I(\gamma_{ijk})$ *be an invariant (under the group* G *which leaves unaltered the canonical form) of total weight* $w^{(i)}$ *in the units of* B_i. *If we subject the units of* E *to the transformation*

$$e_{i_p}' = \sum_{q=p}^{\alpha-1} \sum_{j_q} a_{i_p j_q} e_{j_q}$$

(belonging to G*) whose determinant* $A = \prod_{p=1}^{\alpha-1} A_p \neq 0$, *where*

$$A_p = |a_{i_p j_p}|,$$

then

$$I(\gamma'_{ijk}) \equiv \prod_{p}^{1, \alpha-1} A_p{}^{r_p} I(\gamma_{ijk}),$$

where the γ'*s are the constants of multiplication of the transformed algebra, and where*

$$r_p = \frac{w^{(p)}}{n^{(p)}}.$$

§ 5. Finiteness of rational, integral invariants of nilpotent algebras of genus (3; 2, 1) in canonical form. The multiplication table of the general nilpotent algebra of genus (3; 2, 1) in canonical form is

$$e_i e_j = \gamma_{ij3} e_3 \quad (i, j = 1, 2), \qquad e_k e_3 = 0 = e_3 e_k \quad (k = 1, 2, 3),$$

and here the transformations of the group G are of the form

T:

$$e_i' = \sum_{j}^{1, 3} a_{ij} e_j \qquad (i = 1, 2),$$

$$e_3' = a_{33} e_3 \qquad a_{33}(a_{11}a_{22} - a_{12}a_{21}) \neq 0.$$

By the transformation T, the γ's are subjected to the induced transformation

$$\gamma'_{ij3} = \frac{\sum_{k,l} a_{ik} a_{jl} \gamma_{kl3}}{a_{33}} \equiv f_{ij}(\gamma_{kl3}) \qquad (i, j = 1, 2).$$

And thus, by Lie's theory of continuous groups, if a rational, integral function I of the γ's is invariant under T, I must be annihilated by the two operators

$$U_{12} \equiv (\gamma_{123} + \gamma_{213}) \frac{\partial}{\partial \gamma_{113}} + \gamma_{223} \left(\frac{\partial}{\partial \gamma_{123}} + \frac{\partial}{\partial \gamma_{213}} \right),$$

$$U_{21} \equiv (\gamma_{123} + \gamma_{213}) \frac{\partial}{\partial \gamma_{223}} + \gamma_{113} \left(\frac{\partial}{\partial \gamma_{123}} + \frac{\partial}{\partial \gamma_{213}} \right),$$

and all gradients so annihilated are invariants.* The theory of § 4 tells us that there are no absolute rational, integral invariants.

Now is there only a finite number of rational, integral invariants in the sense that all such invariants are expressible as polynomials in a finite number of them? By analogy with the theory of the Aronhold operators in the study of invariants of algebraic forms, we answer this question by considering the commutator

$$\begin{aligned} (U_{12}, U_{21}) &\equiv U_{12}U_{21} - U_{21}U_{12} \\ &\equiv 2\left(\gamma_{223} \frac{\partial}{\partial \gamma_{223}} - \gamma_{113} \frac{\partial}{\partial \gamma_{113}} \right) \\ &\equiv 2\left\{ \Sigma \gamma_{ij3} \frac{\partial}{\partial \gamma_{ij3}} - \left[2\gamma_{113} \frac{\partial}{\partial \gamma_{113}} + \gamma_{123} \frac{\partial}{\partial \gamma_{123}} + \gamma_{213} \frac{\partial}{\partial \gamma_{213}} \right] \right\}. \end{aligned} \tag{4}$$

If now, in particular, this operator acts on a gradient $\mathfrak{G}$ of degree d, we have

$$(U_{12}, U_{21})\mathfrak{G} \equiv 2d\mathfrak{G} - 2\Sigma(2r_{11} + r_{12} + r_{21})\mathfrak{G}$$

where r_{ij} is the degree of any particular term in γ_{ij3}. But $2r_{11} + r_{12} + r_{21}$ is constant for any gradient, since it equals w_1 the weight in e_1. Thus

$$(U_{12}, U_{21})\mathfrak{G} \equiv 2[d - w_1]\mathfrak{G} \tag{5}$$

and also

$$(U_{12}, U_{21})\mathfrak{G} \equiv -2[d - w_2]\mathfrak{G}. \tag{5'}$$

If $w_1 = w_2$ (as is necessarily the case for an invariant), then

$$(U_{12}, U_{21})\mathfrak{G} = 0,$$

which checks with the fact that an invariant is annihilated by U_{12} and U_{21}.

In particular, if $\mathfrak{G}$ is such that $U_{12}\mathfrak{G} = 0$, then from (5) we have

$$U_{12}U_{21}^{p}\mathfrak{G} = 2\left[p(d - w_1) - \sum_{i=1}^{p-1} i \right] U_{21}^{p-1}\mathfrak{G} \quad (p = 1, 2, \cdots). \tag{6}$$

But $U_{21}\mathfrak{G}$ is a gradient whose weight in e_2 is one less than the corresponding

* The proof of this proceeds exactly as the proof of the analogous theorem in the theory of algebraic invariants, as in Elliott, Algebra of Quantics, 2d ed., p. 113. It also follows from the Lie theory, as in Lie, Transformationsgruppen, p. 215, or Cohen, Lie Theory of One-Parameter Groups.

weight of $\mathfrak{G}$, and accordingly there is some positive integer r such that $U_{21}^{r}\mathfrak{G} = 0$. Hence we have

$$0 = 2\left[r(d - w_1) - \sum_{i=1}^{r-1} i \right] U_{21}^{r-1}\mathfrak{G}. \tag{6'}$$

If $d < w_1$, then $p(d - w_1) - \sum_{i=1}^{p-1} i < 0$ for every p and therefore (6′) shows that $U_{21}^{r-1}\mathfrak{G} \equiv 0$ which, in view of (6), implies that $\mathfrak{G} \equiv 0$. Thus we have

Theorem III. *For genus* (3; 2, 1), *if* $\mathfrak{G}$ *is a gradient of degree* d *and of weights* w_1 *and* w_2 *in* e_1 *and* e_2 *respectively, which is annihilated by* U_{12}, *then* $d - w_1 \geq 0$, *which is equivalent to* $w_2 - w_1 \geq 0$. *Similarly, if* $\mathfrak{G}$ *is annihilated by* U_{21}, *then* $d - w_2 \geq 0$ *which is equivalent to* $w_1 - w_2 \geq 0$.

From this theorem we have immediately

Theorem IV. *For genus* (3; 2, 1) *a gradient* $\mathfrak{G}$ *of degree* d *and weights* w_1 *and* w_2 *in* e_1 *and* e_2 *respectively, which is such that* $w_1 = w_2$ *and which is annihilated by* U_{12} (*or by* U_{21}), *is an invariant under the group* G.

For if $U_{12}\mathfrak{G} \equiv 0$, then from (5) we have at once $U_{12}U_{21}\mathfrak{G} \equiv 0$; and hence either $U_{21}\mathfrak{G} \equiv 0$ or $U_{21}\mathfrak{G}$ is a gradient of weights w_1' and w_2' such that $w_1' > w_2'$.

If $\mathfrak{G}$ is a gradient of degree d and weights w_1 and w_2, then (5) gives at once

$$(U_{12}U_{21}^{2} - U_{21}^{2}U_{12})\mathfrak{G} \equiv 2[2(d - w_1) - 1]U_{21}\mathfrak{G};$$

and in general, for every positive integer r,

$$(U_{12}U_{21}^{r} - U_{21}^{r}U_{12})\mathfrak{G} \equiv 2\left[r(d - w_1) - \sum_{i=1}^{r-1} i \right] U_{21}^{r-1}\mathfrak{G}. \tag{7}$$

Furthermore

$$U_{12}^{r}U_{21}^{r}\mathfrak{G} \equiv U_{12}U_{21}\prod_{j=2}^{r}\left\{ U_{12}U_{21} + 2\left[(j-1)(d - w_1) - \sum_{i=1}^{j-1} i \right] \right\}\mathfrak{G}.$$

If $\mathfrak{G}$ be of weight w_2 in e_2, then $U_{21}^{w_2+1}\mathfrak{G} \equiv 0$, and accordingly $U_{12}U_{21}$ annihilates

$$\prod_{j=1}^{w_2}\left\{ U_{12}U_{21} + 2\left[j(d - w_1) - \sum_{i=1}^{j} i \right] \right\}\mathfrak{G}. \tag{8}$$

If, in particular, $\mathfrak{G}$ is such that $w_1 = w_2 = d$, then (8) is a gradient whose weight in e_1 equals its weight in e_2, and therefore the result of operating U_{21} on (8) is identically zero or is a gradient whose weight in e_1 is greater than its weight in e_2. Hence, by Theorem III, U_{21} annihilates expression (8); and consequently, by Theorem IV, we have

Theorem V. *The operator*

$$\prod_{j=1}^{\infty}\left\{ \frac{U_{12}U_{21}}{2\sum_{i=1}^{j} i} - 1 \right\}$$

when applied to any gradient of a nilpotent algebra of genus (3; 2, 1) *in canonical form, for which* $w_1 = w_2$, *produces a function which is invariant under the group* G. *When applied to an invariant under* G, *this operator produces the invariant itself.*

We are now in a position to show that, for a nilpotent algebra of genus (3; 2, 1) in canonical form, all rational integral invariants under the group G are expressible rationally and integrally in a finite number of such invariants. For by Hilbert's Theorem about an infinite sequence of polynomials,* any such rational integral invariant I is expressible in the form

$$I \equiv \sum_{j}^{1, m} C_j I_j,$$

where m is a finite number, and where the I_j are rational integral invariants, the same for every invariant I. Since I and the I_j are gradients for which $w_1 = w_2$, we may suppose that the C_j are also. Applying Theorem V, we have

$$I \equiv \sum_{j}^{1, m} I_j' I_j,$$

where the I_j' are invariants for genus (3; 2, 1) in canonical form. Then by induction we have

Theorem VI. *For nilpotent algebras of genus* (3; 2, 1) *in canonical form, the rational integral invariants under the group* G *leaving unaltered the canonical form are polynomials in a finite number of such invariants, called the fundamental invariants.*

§ 6. **Fundamental rational, integral invariants for genus (3; 2, 1).** Since any rational, integral invariant under the group G must be annihilated by the operators U_{12} and U_{21} of § 5, it follows immediately that there is essentially only one linear invariant here, namely $\gamma_{123} - \gamma_{213}$, which vanishes for commutative algebras and no others. All quadratic invariants are linear combinations of the square of the linear invariant and $\gamma_{113}\gamma_{223} - \gamma_{123}\gamma_{213}$, the determinant of the (covariant)† bilinear form. As the only cubic invariants are functions of these, we would suspect that these are the fundamental invariants.‡

By the theory of rational, integral invariants for algebraic forms, we know that the determinant $D \equiv |\gamma_{ij3}|$ $(i, j = 1, 2)$ is the only invariant for the quadratic form $\sum_{i,j}^{1, 2} \gamma_{ij3} x_i x_j$ $(\gamma_{ij3} = \gamma_{ji3})$ in the sense that all other such

* "Ueber die Theorie der algebraischen Formen," Mathematische Annalen, vol. 36, p. 474.

† Author's dissertation, § 11.

‡ That is, for the field of rational numbers, for the field of reals, or for the field of ordinary complex numbers.

invariants are expressible as polynomials in it. But this quadratic form is a covariant,* under the group G, of the nilpotent algebra of genus (3; 2, 1) in canonical form; and thus, translating our knowledge of D over to the invariants for the linear algebra, we see that, when $\gamma_{ij3} = \gamma_{ji3}$, the only rational integral invariants of the general nilpotent algebra of genus (3; 2, 1) in canonical form become polynomials in $\gamma_{113}\gamma_{223} - \gamma_{123}\gamma_{213}$. In other words, every rational integral invariant for genus (3; 2, 1) is of the form

$$aD^p + (\gamma_{123} - \gamma_{213})\phi, \tag{9}$$

where ϕ is homogeneous and of degree $2p - 1$ in the γ's. But $\gamma_{123} - \gamma_{213}$ is an invariant for this genus and hence so also is ϕ. Thus by induction we have

Theorem VII. *Under the group G, every rational integral invariant of the nilpotent algebra of genus* (3; 2, 1) *in canonical form is a polynomial in* $\gamma_{113}\gamma_{223} - \gamma_{123}\gamma_{213}$ *and* $\gamma_{123} - \gamma_{213}$.

§ 7. Finiteness of rational, integral invariants for genus (3; 3, 1). For genus (3; 3, 1) the canonical form is

$$e_ie_j = \gamma_{ij4}e_4 \quad (i, j = 1, 2, 3), \qquad e_4e_k = 0 = e_ke_4 \quad (k = 1, \cdots, 4),$$

the transformations of the group G are of the form

$$e_i' = \sum_j^{1,4} a_{ij}e_j \qquad (i = 1, 2, 3),$$

$$e_4' = a_{44}e_4, \qquad a_{44}|a_{ij}| \neq 0 \qquad (i, j = 1, 2, 3),$$

and the constants of multiplication are subject to the induced transformation

$$\gamma'_{ij4} = \frac{1}{a_{44}} \sum_{k,l}^{1,3} a_{ik}a_{jl}\gamma_{kl4} \equiv f_{ij}(\gamma_{kl4}) \qquad (i, j = 1, 2, 3).$$

Here the annihilators are

$$U_{12} \equiv (\gamma_{124} + \gamma_{214})\frac{\partial}{\partial\gamma_{114}} + \gamma_{224}\frac{\partial}{\partial\gamma_{124}} + \gamma_{234}\frac{\partial}{\partial\gamma_{134}} + \gamma_{224}\frac{\partial}{\partial\gamma_{214}} + \gamma_{324}\frac{\partial}{\partial\gamma_{314}},$$

$$U_{13} \equiv (\gamma_{134} + \gamma_{314})\frac{\partial}{\partial\gamma_{114}} + \gamma_{324}\frac{\partial}{\partial\gamma_{124}} + \gamma_{334}\frac{\partial}{\partial\gamma_{134}} + \gamma_{234}\frac{\partial}{\partial\gamma_{214}} + \gamma_{334}\frac{\partial}{\partial\gamma_{314}},$$

together with the operators U_{21}, U_{23}, U_{31} and U_{32} obtained from these two by a permutation of the subscripts 1, 2, 3.

By § 4, there are no linear nor quadratic invariants here; in fact an invariant must be of degree three or a multiple of three. All cubic invariants are linear combinations of

$$|\gamma_{ij4}| \qquad (i, j = 1, 2, 3), \tag{10}$$

* Author's dissertation, § 11.

the discriminant of the (covariant) bilinear form $\sum_{i,j}^{1,3} \gamma_{ij4} x_i y_j$, and

$$\Sigma\gamma_{114}(\gamma_{234} - \gamma_{324})^2 + \Sigma\gamma_{124}\gamma_{314}(\gamma_{234} - \gamma_{324}), \tag{10'}$$

which vanishes for commutative algebras. By analogy with genus (3; 2, 1) we would surmise that these are the fundamental invariants. To show that such is the case, we will base our work on our knowledge of genus (3; 2, 1).

By the same kind of argument as that used in § 6, we know that any invariant for genus (3; 3, 1) is of the form

$$a|\gamma_{ij4}|^p + \chi(\gamma_{kl4}), \qquad i, j = 1, 2, 3, \tag{11}$$

where χ vanishes when $\gamma_{ij4} - \gamma_{ji4} = 0$ $(i, j = 1, 2, 3)$. But any invariant for the general algebra under the total group G is invariant under the group of transformations

$$\begin{aligned} e_i' &= \sum_{j=1}^{2} a_{ij} e_j \qquad (i = 1, 2), \\ e_3' &= \sum_{j=1}^{3} a_{3j} e_j, \\ e_4' &= a_{44} e_4, \end{aligned} \tag{12}$$

where

$$a_{33}a_{44}(a_{11}a_{22} - a_{12}a_{21}) \neq 0.$$

Hence, if

$$\gamma_{134} - \gamma_{314} = 0 = \gamma_{234} - \gamma_{324}, \tag{13}$$

any invariant for genus (3; 3, 1) has the invariantive property for (e_1, e_2, e_4) —a general algebra of genus (3; 2, 1)—after γ'_{134}, γ'_{234} and γ'_{334} are replaced by their expressions in terms of the γ_{ij4}, no matter what be the values of γ_{134}, γ_{234} and γ_{334}.

For an algebra of genus (3; 3, 1) where (13) is satisfied, any invariant (11) becomes

$$a|\gamma_{ij4}|^p + \chi'(\gamma_{kl4}), \qquad i, j = 1, 2, 3, \tag{11'}$$

where χ' vanishes when $\gamma_{124} = \gamma_{214}$. Now in χ' there are no terms in γ_{134} $(= \gamma_{314})$ or γ_{234} $(= \gamma_{324})$. This can be shown quickly by considering the parastrophic algebra, or by the following elementary proof by induction.

Suppose that in χ', of the terms containing γ_{334} to a power greater than h, there are none actually containing γ_{134} or γ_{234}; and consider that term which contains γ_{134} to the kth power and no higher,

$$\gamma_{334}^h \gamma_{134}^k \gamma_{234}^l \psi, \tag{14}$$

where ψ is independent of γ_{134} $(= \gamma_{314})$ and γ_{234} $(= \gamma_{324})$. By Lemma 1, there is only one such term.

If we subject the algebra to the transformation

$$e_i' = e_i \qquad (i \neq 3),$$
$$e_3' = e_1 + e_3,$$

the γ's are subjected to the transformation

$$\gamma'_{ij4} = \gamma_{ij4} \qquad (i, j = 1, 2),$$
$$\gamma'_{134} = \gamma_{114} + \gamma_{134},$$
$$\gamma'_{314} = \gamma_{114} + \gamma_{314},$$
$$\gamma'_{234} = \gamma_{214} + \gamma_{234},$$
$$\gamma'_{324} = \gamma_{124} + \gamma_{324},$$
$$\gamma'_{334} = \gamma_{114} + \gamma_{134} + \gamma_{314} + \gamma_{334}.$$

Since ψ is of weight zero in e_3, (14) for $(k, l) \neq (0, 0)$ is replaced by

$$\gamma_{334}^{h}[\gamma_{134}^{k}\gamma_{234}^{l} + \gamma_{114}^{k}\gamma_{214}^{l} + \alpha]\psi + \beta\psi,$$

where α contains only terms whose weight in e_1 is less than $2k + l$, the weight of $\gamma_{114}^{k}\gamma_{214}^{l}$, and where β does not involve γ_{334} to a power as high as h. Since χ' is unaltered under this transformation for all values of γ_{334}, γ_{134} $(= \gamma_{314})$ and γ_{234} $(= \gamma_{324})$ after the γ'_{ijk} have been replaced by their expressions in terms of the γ_{ijk}, then in χ' there must be a term to cancel $\gamma_{334}^{h}\gamma_{114}^{k}\gamma_{214}^{l}\psi$, if $\psi \neq 0$, $(k, l) \neq (0, 0)$. But the only terms of χ' (γ'_{ijk}) which will contribute terms containing γ_{334}^{h} are those containing $\gamma_{334}^{\prime g}$ $(g \geq h)$. By the hypothesis about h and Lemma 1, $g = p$. But $\gamma_{334}^{\prime p}\psi_p$ contributes only the term $\gamma_{334}^{h}\gamma_{114}^{p-h}\psi_p$ which might cancel $\gamma_{334}^{h}\gamma_{114}^{k}\gamma_{214}^{l}\psi$. Thus $p - h \leq k$. Also $2p = 2h + k + l$, since χ' is isobaric in e_3; and hence $k \geq l$. Similarly $l \geq k$; and accordingly $k = l$.

Now apply to the algebra the transformation

$$e_1' = e_1 + e_2, \tag{15}$$
$$e_i' = e_i \qquad (i \neq 1).$$

Then, since χ' is absolutely unaltered under (15), any term of the form

$$\gamma_{334}^{\prime h}\gamma_{134}^{\prime k}\gamma_{234}^{\prime k}\psi(\gamma')$$

for $k > 0$ contributes the term

$$\gamma_{334}^{h}\gamma_{234}^{2k}\psi(\gamma)$$

which must be cancelled. Hence, since there is no term which could possibly cancel this when $k > 0$, $\psi \not\equiv 0$, we must have finally that $k = l = 0$, if $\psi \not\equiv 0$.

Accordingly the invariant χ, of degree $3p$, when (13) is satisfied becomes the product of γ_{334}^p by a function of degree $2p$ which is invariant for the subalgebra (e_1, e_2, e_4) of genus $(3; 2, 1)$. Hence, by Theorem VII, we deduce

Lemma IV. *For nilpotent algebras of genus* $(3; 3, 1)$ *in canonical form, any rational integral invariant under the group G is necessarily of the form*

$$I = a|\gamma_{ij4}|^p + \chi(\gamma_{kl4})$$

where

$$\chi \equiv \sum_3 \left(\sum_{q=1}^{p} a_q \gamma_{334}^p (\gamma_{124} - \gamma_{214})^{2q} (\gamma_{114}\gamma_{224} - \gamma_{124}\gamma_{214})^{p-q} \right)^* + \theta,$$

where θ *is rational, integral and homogeneous in the* γ*'s and vanishes when any one of the three conditions*

$$\gamma_{124} - \gamma_{214} = 0 = \gamma_{134} - \gamma_{314}$$

$$\gamma_{214} - \gamma_{124} = 0 = \gamma_{234} - \gamma_{324}$$

$$\gamma_{314} - \gamma_{134} = 0 = \gamma_{324} - \gamma_{234}$$

is satisfied.

Applying this lemma to the case where $w^{(1)} = 6$, we have

$$\chi = b \sum_3 \gamma_{114}(\gamma_{234} - \gamma_{324})^2 + c \sum_6 \gamma_{124}\gamma_{234}(\gamma_{134} - \gamma_{314}).$$

Since χ must be invariant under the transformation

$$e_1' = e_1 + xe_2,$$

$$e_i' = e_i \qquad (i \neq 1),$$

where x is arbitrary, we have $c = -b$, which agrees with the first part of this section.

In any invariant of the nilpotent algebra of genus (3; 3, 1), we can kill off the terms of the form

$$\Sigma\gamma_{334}^p(\gamma_{124} - \gamma_{214})^{2q}(\gamma_{114}\gamma_{224} - \gamma_{124}\gamma_{214})^{p-q}$$

one by one by means of

$$|\gamma_{ij4}|^{p-q}[\Sigma\gamma_{334}(\gamma_{124} - \gamma_{214})^2 - \Sigma\gamma_{124}\gamma_{234}(\gamma_{134} - \gamma_{314})]^q$$

and thus we obtain an invariant K which vanishes when any one of the three conditions

$$\gamma_{124} - \gamma_{214} = 0 = \gamma_{134} - \gamma_{314},$$

(16)

$$\gamma_{214} - \gamma_{124} = 0 = \gamma_{234} - \gamma_{324},$$

$$\gamma_{314} - \gamma_{134} = 0 = \gamma_{324} - \gamma_{234}$$

is satisfied.

* The first summation sign extends over all permutations of the indices 1, 2, 3 which produce distinct terms of the type indicated.

Now

$$K \equiv \sum_{r,s,t} (\gamma_{124} - \gamma_{214})^r (\gamma_{234} - \gamma_{324})^s (\gamma_{134} - \gamma_{314})^t K_{r,s,t}$$

where each $K_{r,s,t}$ is independent of γ_{124}, γ_{234} and γ_{134} and where $K_{r,0,0} \equiv K_{0,s,0} \equiv K_{0,0,t} \equiv 0$ for every r, s, t, since K vanishes whenever any one of the conditions (16) is satisfied. Consider the set of terms where r has the least value r_0, such that some $K_{r_0,s,t} \not\equiv 0$, and $s + t = q$ has a fixed value. Of these, consider that term where s has the greatest value, s_0. Then the corresponding $K_{r,s,t}$ has its weight in e_2 less than that of any other term of this set.

When we subject the algebra to the transformation (15), then the term

$$(\gamma_{124} - \gamma_{214})^{r_0} (\gamma_{234} - \gamma_{324})^{s_0} (\gamma_{134} - \gamma_{314})^{t_0} K_{r_0,s_0,t_0} \qquad (s_0 + t_0 = q),$$

if $t_0 \neq 0$, is replaced by

$$(\gamma_{124} - \gamma_{214})^{r_0} [(\gamma_{234} - \gamma_{324})^{s_0} (\gamma_{134} - \gamma_{314})^{t_0} K_{r_0,s_0,t_0} + (\gamma_{234} - \gamma_{324})^q K_{r_0,s_0,t_0} + \alpha],$$

where no term of α can cancel $(\gamma_{234} - \gamma_{324})^q K_{r_0,s_0,t_0}$. Since K is invariant under (15), the term $(\gamma_{124} - \gamma_{214})^{r_0} (\gamma_{234} - \gamma_{324})^q K_{r_0,s_0,t_0}$ must be cancelled if $K_{r_0,s_0,t_0} \not\equiv 0$, $t_0 \neq 0$. But there is no term in $(\gamma_{124} - \gamma_{214})^{t_0} (\gamma_{234} - \gamma_{324})^q$ which has its weight in e_2 small enough to do this, on account of the way s_0 was chosen; and accordingly we must have $K_{r_0,s_0,t_0} \equiv 0$ if $t_0 \neq 0$.

Thus $\gamma_{134} - \gamma_{314}$ is not a factor of K. But $(\gamma_{124} - \gamma_{214})^{r_0}$ is a factor of K, and accordingly $r_0 = 0$, in view of the invariancy of K under the transformation

$$e_i' = e_i \qquad (i \neq 2, 3),$$

$$e_2' = e_3,$$

$$e_3' = e_2.$$

But by previous remarks, $K_{0,s_0,0} \equiv 0$; and consequently $K_{r_0,s_0,t} \equiv 0$ for every t. Hence, in view of the definition of r_0 and s_0, $K \equiv 0$; and we have

Theorem VIII. *Any rational integral invariant of the nilpotent algebra of genus* (3; 3, 1) *in canonical form is a polynomial in the invariants*

$$|\gamma_{ij4}|_{i,j=1,2,3} \qquad \textit{and} \qquad \sum_3 \gamma_{334}(\gamma_{124} - \gamma_{214})^2 - \sum_6 \gamma_{124}\gamma_{234}(\gamma_{134} - \gamma_{314}).$$

§ 8. Finiteness proof for genus $(\alpha; n', \cdots, n^{(\alpha-1)})$. To prove the finiteness of the rational, integral invariants for the general case, we make use of a theorem which is essentially one proved by Gordan,* F. Mertens,† and Hilbert,‡ and which for $n' = 3$, $n'' = 2$ runs as follows: Let

* "Invariantentheorie," vol. II, § 9.

† Sitzungsberichte der Kais. Akad. der Wiss. zu Wien, vol. 95, p. 942.

‡ L. c., p. 524.

$E = (e_1, e_2, e_3, e_4, e_5)$ be a nilpotent algebra of genus (3; 3, 2) in canonical form where the units are subjected to the transformation

$$(17)\qquad \begin{aligned} e_i' &= \sum_j^{1,5} a_{ij} e_j \qquad (i = 1, 2, 3), \\ e_k' &= \sum_l^{4,5} b_{kl} e_l \qquad (k = 4, 5) \end{aligned}$$

with

$$A_1 \equiv \left| a_{ij} \right|_{i,j=1,2,3} \neq 0, \qquad A_2 \equiv \left| b_{kl} \right|_{k,l=4,5} \neq 0.$$

Let γ_{ijk} and γ'_{ijk} be the constants of multiplication for the original algebra E and the transformed algebra respectively. Finally, let $H(\gamma_{ijk})$ be a rational, integral function of the coefficients of multiplication of E, and let

$$\Omega_a = \sum_{i,j,k} (\pm\, ijk) \frac{\partial^3}{\partial a_{1i} \partial a_{2j} \partial a_{3k}},$$

where the summation extends over all permutations of 1, 2 and 3 and where $(\pm\, ijk)$ denotes $+1$ or -1 according as i, j, k is an even or odd permutation; similarly let

$$\Omega_b \equiv \sum_{f,g} (\pm\, fg) \frac{\partial^2}{\partial b_{4f} \partial b_{5g}},$$

where the summation extends over all permutations of 4 and 5 and where $(\pm\, fg)$ is $+1$ or -1 according as f, g is an odd or an even permutation. Then, if p_1 and p_2 are such that

$$J(\gamma) \equiv \Omega_a^{p_1}\, \Omega_b^{p_2}\, A_1^{q_1}\, A_2^{q_2}\, H(\gamma')$$

is free of the coefficients of the transformation, $J(\gamma)$ is an invariant of the algebra. The proof runs exactly as in Hilbert's article.

Now, by the theorem of Hilbert quoted in § 5, any rational, integral invariant I of the nilpotent algebras of genus (3; 3, 2) in canonical form may be written

$$I(\gamma) \equiv \sum_j^{1,m} C_j(\gamma) I_j(\gamma)$$

where m is a finite number, the I_j are rational, integral invariants for genus (3; 3, 2) the same for every invariant I, and where the C_j are isobaric, rational, integral homogeneous functions of the constants of multiplication. Furthermore, we may take the $C_j(\gamma)$ such that the combined weight of C_j and I_j in B_1 is the weight of I in B_1, and that their combined weight in B_2 is the weight of I in B_2.

When we subject the units to the transformation (17), this equation becomes

$$(18)\qquad A_1^{w^{(1)}} A_2^{w^{(2)}} I(\gamma) \equiv \sum_j^{1,m} A_1^{w_j^{(1)}} A_2^{w_j^{(2)}} C_j(\gamma') I_j(\gamma)$$

where $w^{(1)}$ and $w^{(2)}$ are the total weights of I in the units of B_1 and B_2 respectively, and where $w_j^{(1)}$ and $w_j^{(2)}$ are the total weights of I_j in the units of B_1 and B_2 respectively. Moreover, on account of the way the C_j were chosen, both sides are of the same degree in the a's and in the b's.

Now, unlike the proof of the analogous theorem for invariants of algebraic forms, we can not apply the theorem of Hilbert stated at the beginning of this section directly to (18). For, since $w^{(2)}$ is negative, we can not apply Ω_b to (18) a number of times sufficient to free both sides of the equation from the coefficients of the transformation (17). But, by (3) § 4, each γ' is a rational, integral function of the coefficients of the transformation divided by A_2. If, accordingly, we multiply both sides of (18) by $A_2{}^p$, where p is chosen sufficiently large, we have an equation between two functions which are rational, integral and of the same degree in the a's and in the b's.

If we now operate on the resulting equation with $\Omega_a^{w^{(1)}/\beta}\Omega_b^{-w^{(2)}/\beta'+p}$ we have, by Hilbert's theorem,

$$NI(\gamma) \equiv \sum_j^{1,\,m} I_j'(\gamma) I_j(\gamma),$$

where the I_j' are rational integral invariants, and where N is a constant different from zero. Thus, by induction, we prove the finiteness of the rational, integral invariants for genus (3; 3, 2).

In a similar manner we prove

Theorem IX. *For the nilpotent algebra of genus* $(\alpha;\ n',\ \cdots,\ n^{(\alpha-1)})$ *in canonical form, the rational, integral invariants are expressible as polynomials in a finite number of such invariants.*

BRYN MAWR COLLEGE,
BRYN MAWR, PA.

ON TRIGONOMETRIC SERIES.*

By William LeRoy Hart.

1. Introduction. The present paper is concerned with series of the form

$$(1)\quad f(t) = \sum_{k=0}^{\infty} a_k \cos 2\pi\alpha_k t + b_k \sin 2\pi\alpha_k t \qquad (\alpha_0 = 0,\ \alpha_k > 0;\ k = 1, 2, \cdots),$$

where the α_k $(k = 1, 2, \cdots)$ are not necessarily commensurable, which is a generalization of Fourier series. In problems in applied mathematics where such expressions arise, the $f(t)$ are given by observation of natural phenomena or by experiment; the α_k are in some cases given by theory and, in others, remain to be determined. Thus there are two cases which it is proper to consider; first, that of the determination of the (a_k, b_k) when $f(t)$ and the α_k are given and, second, that of the determination of the (α_k, a_k, b_k) when only the $f(t)$ is known.

An example of the first case is found in the recent determination of the rigidity of the earth by A. A. Michelson† from a consideration of the tidal effects of the sun and moon on the earth. The height of the tide is known to be expansible in the form (1) and, moreover, the mathematical theory of the tides gives the values of the α_k. The determination of the (a_k, b_k) for the principal terms was the main object of the experiment which Michelson carried out.

The variation of sun-spot activity furnishes an example of the second case. The number and dimensions of sun spots vary greatly with the time, and it has been suggested by many astronomers that they may be the result of component periodic causes. In other words, it is suspected that sun-spot activity as a function of the time can be represented in the form (1). The problem then is to find the (α_k, a_k, b_k) from the curve of observation.

In article 2, it is assumed that $f(t)$ is expansible in the form (1) with known α_k and, under certain hypotheses as to the convergence of the series, it is shown how to compute the (a_k, b_k). In article 3 it is then shown that if there exists one expansion for $f(t)$ satisfying the conditions of article 2, this expansion is unique.

Professor A. Schuster has introduced the method of periodogram analysis for the determination of the periods of the unknown factors which enter into a certain compound periodic effect. In article 4, the results of the present paper are connected with a certain phase of Schuster's work.

* Presented to the American Mathematical Society at Chicago, April 12, 1914.

† Astrophysical Journal, vol. 39 (1914), p. 105.

2. Determination of the Coefficients. The results of this article are stated in the following

Theorem I. *Let there be given the series*

$$F(t) = \sum_{n=0}^{\infty} A_n \phi_n(2\pi\alpha_n t) \qquad (\phi_0 = 1,\ \alpha_n > 0), \tag{2}$$

where $\phi_n(\theta)$ represents either sin θ or cos θ. Then, if

$$\sum_{n=0}^{\infty} |A_n| \tag{3}$$

converges, it follows that

$$A_i = 2\alpha_i \lim_{k=\infty} \frac{1}{k} \int_0^{k\,\alpha_i} F(t)\phi_i(2\pi\alpha_i t)dt \qquad (i = 1, 2, \cdots),$$

$$A_0 = \delta \lim_{k=\infty} \frac{1}{k} \int_0^{k\,\delta} F(t)dt \qquad (\delta > 0).$$

In the proof of this theorem there is needed the

Lemma 1. *If $\alpha > 0$, $\beta > 0$ and $\beta \neq m\alpha$ (m an integer), then*

$$\lim_{k=\infty} \frac{1}{k+1} \sum_{j=0}^{k} \phi\left[2\pi\beta\left(t + \frac{j}{\alpha}\right)\right] = 0,$$

uniformly for all t.

Let the proof of the lemma be considered only for the case when $\phi(\theta)$ is *cos* θ. The reasoning is similar for the case when $\phi(\theta) = \sin\theta$. Let

$$\begin{aligned} P_k(t) &= \sum_{j=0}^{k} \phi\left[2\pi\beta\left(t + \frac{j}{\alpha}\right)\right] = \sum_{j=0}^{k} \cos 2\pi\beta\left(t + \frac{j}{\alpha}\right), \\ &= \cos 2\pi\beta t \sum_{j=0}^{k} \cos\frac{2j\pi\beta}{\alpha} - \sin 2\pi\beta t \sum_{j=1}^{k} \sin\frac{2j\pi\beta}{\alpha}. \end{aligned} \tag{4}$$

By means of the trigonometric identities

$$\frac{1}{2} + \sum_{j=1}^{k} \cos jx = \frac{\cos kx - \cos(k+1)x}{2(1 - \cos x)} \qquad (x \neq 2m\pi),$$

$$\sum_{j=1}^{k} \sin jx = \frac{\sin kx - \sin(k+1)x + \sin x}{2(1 - \cos x)} \qquad (x \neq 2m\pi),$$

equation (4) becomes

$$\begin{aligned} P_k(t) = &\frac{\cos 2\pi\beta t}{2\left(1 - \cos\frac{2\pi\beta}{\alpha}\right)}\left[1 - \cos\frac{2\pi\beta}{\alpha} + \cos k\frac{2\pi\beta}{\alpha} - \cos(k+1)\frac{2\pi\beta}{\alpha}\right] \\ &- \frac{\sin 2\pi\beta t}{2\left(1 - \cos\frac{2\pi\beta}{\alpha}\right)}\left[\sin k\frac{2\pi\beta}{\alpha} - \sin(k+1)\frac{2\pi\beta}{\alpha} + \sin\frac{2\pi\beta}{\alpha}\right]. \end{aligned} \tag{5}$$

LIBRARY
LELAND STANFORD JUNIOR
UNIVERSITY

From (5) it is seen that

$$|P_k(t)| \leqq \frac{7}{2\left|1 - \cos\frac{2\pi\beta}{\alpha}\right|} = M \qquad (k = 1, 2, \cdots; 0 \leqq t < \infty),$$

and therefore the lemma follows immediately.

To establish the theorem, it will first be proved that *if* $K_i(t)$ *represents the sum of all terms of* $F(t)$ *with* $\alpha_h = m_h\alpha_i$ (m_h *an integer*), *then*

$$\lim_{k=\infty} \frac{1}{k}\sum_{j=0}^{k-1} F\left(t + \frac{j}{\alpha_i}\right) = K_i(t), \tag{6}$$

uniformly for all t.

From the definition of $K_i(t)$ it follows that

$$K_i(t) = \sum_{h=0}^{\infty} C_h\psi_h(2\pi m_h\alpha_i t)$$

($\psi_h(\theta)$ *is either sin* θ *or cos* θ), where the C_h are a subset of the A_n; therefore since $\sum_{h=0}^{\infty}|C_h|$ exists, $K_i(t)$ is uniformly convergent for all t. Moreover, K_i has the period $1/\alpha_i$. Hence it is seen that

$$\frac{1}{k}\sum_{j=0}^{k-1} K_i\left(t + \frac{j}{\alpha_i}\right) = K_i(t) \qquad (i = 1, 2, \cdots). \tag{7}$$

In view of (7) and the absolute convergence of all series involved, it follows that

$$\begin{aligned} \left|\frac{1}{k}\sum_{j=0}^{k-1} F\left(t + \frac{j}{\alpha_i}\right) - K_i(t)\right| &= \left|\frac{1}{k}\sum_{j=0}^{k-1}\left[F\left(t + \frac{j}{\alpha_i}\right) - K_i\left(t + \frac{j}{\alpha_i}\right)\right]\right|, \\ &= \left|\frac{1}{k}\sum_{j=0}^{k-1} H_i\left(t + \frac{j}{\alpha_i}\right)\right|, \end{aligned} \tag{8}$$

where $H_i(t)$ is the sum of all terms of $F(t)$ not contained in $K_i(t)$.

To establish (6) it must be shown that, for every value $l > 0$, expression (8) is at most equal to l if $k \geqq k_l$ (k_l chosen sufficiently large). It is easily verified that

$$H_i(t) = \sum_{m=0}^{\infty} D_m\Phi_m(2\pi\gamma_m t) \qquad (\gamma_m \neq p_m\alpha_i;\ p_m \text{ an integer}),$$

where the (D_m) are a subset of the (A_n) and where $\Phi_m(\theta)$ represents either $\sin\theta$ or $\cos\theta$. Therefore $H_i(t)$ converges uniformly for all t. Hence for every $l > 0$, h can be chosen so large that

$$\left|\sum_{m=h+1}^{\infty} D_m\Phi_m(2\pi\gamma_m t)\right| \leqq \frac{l}{2} \qquad (0 \leqq t < \infty). \tag{9}$$

LIBRARY
LELAND STANFORD JUNIOR
UNIVERSITY

By use of (9) and by an application of Lemma (1) to each term of $\sum_{m=0}^{h} D_m \Phi_m(2\pi\gamma_m t)$, it follows that k_l can be chosen so large that expression (8) is at most l for all values of t. Hence (6) is established.

From the definition of $K_i(t)$ it follows that $A_i\phi_i(2\pi\alpha_i t)$ is one of its terms. Therefore, by the theory of Fourier series, it is seen that

$$A_i = 2\alpha_i \int_0^{1/\alpha_i} K_i(t)\phi_i(2\pi\alpha_i t)dt.$$

Since the limit in (6) exist niformly, it follows that

$$\begin{aligned} A_i &= 2\alpha_i \int_0^{1/\alpha_i} \left\{ \lim_{k=\infty} \frac{1}{k} \sum_{j=0}^{k-1} F\left(t + \frac{j}{\alpha_i}\right) \phi_i\left[2\pi\alpha_i\left(t + \frac{j}{\alpha_i}\right)\right] \right\} dt, \\ &= 2\alpha_i \lim_{k=\infty} \frac{1}{k} \int_0^{1/\alpha_i} \sum_{j=0}^{k-1} F\left(t + \frac{j}{\alpha_i}\right) \phi_i\left[2\pi\alpha_i\left(t + \frac{j}{\alpha_i}\right)\right] dt, \\ &= 2\alpha_i \lim_{k=\infty} \frac{1}{k} \int_0^{k/\alpha_i} F(t)\phi_i(2\pi\alpha_i t)dt, \end{aligned}$$

which is the result stated in the theorem.

Now consider the constant term in (2). For every given $\delta > 0$, the expression $K_\delta(t)$, the sum of the terms of $F(t)$ with α_n a multiple of δ, has A_0 as its constant term. Hence it follows that, for every $\delta > 0$,

$$A_0 = \delta \int_0^{1/\delta} K_\delta(t)dt = \delta \lim_{k=\infty} \frac{1}{k} \int_0^{k/\delta} F(t)dt.$$

It is natural to inquire what sort of functions can be expanded in the form (2). Results of a negative character are obtained in the present paper in regard to this question.

Corollary (1). *If $F(t)$ is such that $|F(t)|$ is integrable to infinity, then, unless F is identically zero, it cannot be expanded in the form* (2).

The corollary results from the fact that, for such a function F, all the coefficients in the expansion would be zero, as can be seen from the values as given in the theorem. By similar reasoning, it is seen that

Corollary (2). *If $F(t)\phi_i(2\pi\alpha_i t)$ is integrable to infinity then $A_i = 0$.*

3. Uniqueness of the expansion. In all applications of (2) it is important to know whether two series with different (α_n, A_n) can represent the same function. This question is answered in the negative in

Theorem II. *Suppose that for a given $f(t)$ there are the two expansions satisfying the hypotheses of Theorem I,*

$$f(t) = \sum_{m=0}^{\infty} A_m\phi_m(2\pi\alpha_m t) \qquad (\phi_0 = 1), \tag{10}$$

$$f(t) = \sum_{m=0}^{\infty} B_m\psi_m(2\pi\beta_m t) \qquad (\psi_0 = 1), \tag{11}$$

where $\phi_m(\theta)$ and $\psi_m(\theta)$ represent either sin θ or cos θ. Then it follows that the set (α_m) are merely a permutation of the (β_m) and that the coefficients of corresponding terms are equal. That is, the expansion of a function in the form (2) is unique.

By a computation similar to that used to establish (6), it follows that, because of (10),

$$\lim_{k=\infty} \frac{1}{k} \sum_{j=0}^{k-1} f\left(t + \frac{j}{\theta}\right) = A_0 + F(t, \theta) \qquad (\theta > 0), \tag{12}$$

where $F(t, \theta)$ consists of all terms of the series (10) with α_m an integral multiple of θ. Similarly it is seen that this same expression is equal to

$$B_0 + H(t, \theta), \tag{13}$$

where $H(t, \theta)$ consists of all terms of (11) with β_m an integral multiple of θ. From (12) and (13) for $\theta = \alpha_i$, and $\theta = \beta_j$, there results

$$A_0 = B_0, \qquad H(t, \alpha_i) = F(t, \alpha_i), \qquad H(t, \beta_j) = F(t, \beta_j).$$

Therefore it follows that if there is a term $A_i\phi_i(2\pi\alpha_i t)$ in (10), it is also present in (11); and if $B_j\psi_j(2\pi\beta_j t)$ is a term of (11), it is also a term of (10). Thus the theorem is established.

4. On periodogram analysis. In connection with a study of sun-spot variation, rainfall variation, etc., Schuster* was led to develop the principal of periodogram analysis for the determination of the periodic effects present in the complex resultants which are given by observation of natural phenomena. That is, on assuming that a certain effect can be represented for all values of t in a series of the form (1), Schuster's method has as its purpose the determination of the values of the unknown periods from a consideration of the curve of observation. The method given below is essentially equivalent to that of Schuster. The present treatment contains a set of hypotheses which can be taken as a basis for periodogram analysis and the results are obtained by simple deductions from the results of the preceeding articles.

Let there be given a function $f(t)$ $(0 \leqq t < \infty)$ and suppose that it can be represented in the form (1) in which it is sought to determine the (α_k, a_k, b_k). Let the function $S(\theta)$ be defined by the equations

$$S(\theta) = \lim_{m=\infty} S_m(\theta),$$

$$S_m(\theta) = \frac{2}{m\theta} \left\{ \left[\int_0^{m\theta} f(t) \cos \frac{2\pi t}{\theta} dt \right]^2 + \left[\int_0^{m\theta} f(t) \sin \frac{2\pi t}{\theta} dt \right]^2 \right\}^{\frac{1}{2}}.$$

* Proceedings of the Cambridge Philosophical Society, vol. 18 (1900), p. 107.

Suppose that $\sum_{k=0}^{\infty} |a_k| + |b_k|$ converges. Then it follows that

$$S\left(\frac{1}{\alpha_i}\right) = \sqrt{a_i^2 + b_i^2} \qquad (i = 1, 2, \cdots).$$

Moreover, if $1/\theta \neq \alpha_i$ $(i = 1, 2, \cdots)$, then $S(\theta) = 0$. Hence, the graph of $S(\theta)$, which depends only on the given function $f(t)$, determines the location of the α_i.

In practice it is, of course, impossible to form the function $S(\theta)$, just as it is impossible in general to write down the sum of an infinite series. For example, in dealing with sun-spot variation, there are at hand only the data for the last 160 years. Hence, in practice, all that can be done is to compute the graph of $S_m(\theta)$ where m can be taken large for small values of θ but must be taken small for large values of θ, and is undefined for all values of m if θ is sufficiently large. However, if $S_m(\theta)$ should be graphed for a certain range $(\theta_0 \leqq \theta \leqq \theta_1)$, its form for m sufficiently large would give an indication of the value of $S(\theta)$ for $(\theta_0 \leqq \theta \leqq \theta_1)$. Hence, a maximum of $S_m(\theta)$ at $\theta = a$ shows that $S(a) \neq 0$ and therefore indicates the presence of an α_k in (1) with the value $\alpha_k = 1/a$. The graph of $S_m(\theta)$ for a given function is identical with the periodogram defined by Schuster, and the determination of the periods from the maxima is his method.

UNIVERSITY OF CHICAGO,
March 1, 1916.

SYMMETRIC FUNCTIONS FORMED BY SYSTEMS OF ELEMENTS OF A FINITE ALGEBRA AND THEIR CONNECTION WITH FERMAT'S QUOTIENT AND BERNOULLI'S NUMBERS.*

By H. S. Vandiver.

In a number of different investigations in the theory of numbers we encounter expressions formed by symmetric functions of systems of integers selected from a set $1, 2, \cdots, m$. I give a few known examples. We have the Wilson theorem:

$$(p-1)! \equiv -1 \pmod{p},$$

when p is prime. From the Lagrange congruence

$$(x-1)(x-2)\cdots(x-(p-1)) \equiv x^{p-1}-1 \pmod{p},$$

we find that the elementary symmetric functions formed by the integers $1, 2, \cdots, p-1$, and of dimension less than $p-1$, are all divisible by p.

Sylvester, in his study of Fermat's quotient, arrived at a formula which was given in the following form by Mirimanoff,†

$$q(m) \equiv \sum_{n=1}^{p-1} \frac{x_n}{p-n} \pmod{p},$$

where

$$q(m) = \frac{m^{p-1}-1}{p},$$

$$x_n \equiv \frac{n}{p} \pmod{m} \qquad (0 < x_n \leqq m).$$

This relation may be written

$$q(m) \equiv \sum_{n=1}^{m} x_n C_n \pmod{p},$$

where

$$C_k = \sum_{i} (mi+k)^{p-2},$$

and i ranges so that $mi+k$ represents all the integers of this form which are less than p. Note that the C's consist of symmetric functions formed by systems of integers in arithmetical progression selected from the set $1, 2, \cdots, p-1$.

Kronecker‡ in his investigation of the divisibility of the first factor of

* Presented to the American Mathematical Society at New York, April, 1913, and April, 1916,

† Crelle, vol. 115.

‡ Cf. Hilbert, Die Theorie der Algebraischen Zahlkörpers, p. 430.

the class number of a cyclotomic field, defined by $\theta = e^{\frac{2i\pi}{l}}$, by the prime l, encountered relations from which we may derive the following:

$$\sum_i q_i r^{i(2t-1)} \equiv \frac{(r^{2t}-1)b_{2t}}{2tr^{2t-1}} \pmod{l},$$

where

$$t < \frac{l-1}{2}, \qquad q_i = \frac{rr_i - r_{i+1}}{l},$$

r being a primitive root of l, $b_1 = -\frac{1}{2}$, $b_{2a+1} = 0$, $b_{2a} = (-1)^{a+1}B_a$, $a > 0$. The B's are the numbers of Bernoulli and r_i is the least positive residue of r^i, modulo l.

In an article on Fermat's last theorem* the writer has derived from a theorem due to Frobenius the relation

$$\frac{b_a(1-k^a)}{a} \equiv \sum_{i=1}^{k-1} \frac{f_a(\alpha^i)}{1-\alpha^{-i}} \pmod{l},$$

for $1 < a < l-1$, α a primitive kth root of unity, $f_a(\alpha^i) = \sum_{r=1}^{l-1} r^{a-1}\alpha^{ir}$, and $1 < k < l$. In the present paper, a few theorems will be given which serve as a basis for deriving as special cases all the results mentioned above as well as some generalizations.

Symmetric functions in a general finite algebra.

1. A finite algebra† is defined as a finite set of elements which may be combined by addition, subtraction and multiplication, subject to the commutative, associative, and distributive laws of ordinary algebra, such that the sum, difference or product of any two elements is uniquely determined as an element of the set, and in which also occurs an element playing the rôle of unity under multiplication. It is shown that every algebra of this type contains a set of m elements called integral elements. The integer m is called the base of the algebra A. Consider a set of elements in A, say

$$n_1, n_2, \cdots, n_k,$$

which has the property that there exists in A an element n (not unity) such that

$$nn_1, nn_2, \cdots, nn_k,$$

is a permutation of the original set. Such a system will be termed a *conjugate set* in the finite algebra A. The number n will be referred to as a multiplier of the set.

* Crelle, vol. 144, p. 314.

† Vandiver, Transactions Amer. Math. Society, vol. 13, p. 293.

Consider an I.H.S.F. (integral homogeneous symmetric function) formed by a conjugate set, say

$$S(n_1, n_2 \cdots n_k).$$

By definition of n, we have

$$S(nn_1, nn_2, \cdots, nn_k) = S = n^d S,$$

and

$$(n^d - 1)S = 0, \tag{1}$$

d being the dimension of the function S. Now if it is possible to select n and d so that $n^d - 1$ is a unit in A, then $S = 0$. This can be done in a number of special cases. We have, if t is the totient of A,*

$$n^t = 1$$

in the algebra. Assume that n and $n - 1$ are units in A, and that d is prime to t. Then it may be shown that $n^d - 1$ is a unit in A. For if $n^d - 1 \equiv 0 \pmod{N}$, where N is a non unit, then we also have

$$n^t - 1 \equiv 0 \pmod{N}.$$

If n belongs to the exponent e modulo N, then $t \equiv 0 \pmod{e}$, as is easily seen, and also $d \equiv 0 \pmod{e}$. Hence, since d is prime to t, we have $e = 1$, but this gives $n - 1 \equiv 0 \pmod{N}$, contrary to definition. Hence $n^d - 1$ is a unit and we have from (1),

Theorem I. *Any* I.H.S.F. *formed by the elements of a conjugate set in a finite algebra A, whose degree is prime to the totient of A, is zero in A, provided there exists a multiplier n of the set such that $n(n - 1)$ is a unit in A.*

Symmetric functions of systems of residues of an ideal modulus.

2. A complete system of residues with respect to an ideal modulus represents a finite algebra. We shall consider this type of algebra in detail with regard to symmetric functions. A C.S.U.R. (complete system of unit residues) modulo $\mathfrak{m}$, an ideal in an algebraic field Ω, is reproduced if each element of the system is multiplied by an integer ρ in Ω which is prime to $\mathfrak{m}$.†

Let

$$\mathfrak{m} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_k^{a_k},$$

where the $\mathfrak{p}$'s are distinct prime ideals in Ω, and let S be an I.H.S.F. of the C.S.U.R. modulo $\mathfrak{m}$. Multiplication by ρ gives (if d is the degree of S) $\rho^d S$, and also S, modulo $\mathfrak{m}$. Hence

$$S(\rho^d - 1) \equiv 0 \pmod{\mathfrak{m}}. \tag{1a}$$

* Vandiver, Transactions Amer. Math. Society, vol. 13, p. 294.

† Dirichlet-Dedekind, Zahlentheorie (4th edition), p. 570.

Now assume that d is not a multiple of $\varphi(\mathfrak{p}_1)$, where $\varphi(\mathfrak{p}_1)$ represents the indicator of $\mathfrak{p}_1$, and let ρ_1 be a primitive root of $\mathfrak{p}_1$. Then

$$d = r\varphi(\mathfrak{p}_1) + d_1,$$

where $0 < d_1 < \varphi(\mathfrak{p}_1)$, and we have

$$\rho_1^{d_1} \not\equiv 1 \pmod{\mathfrak{p}_1}.$$

Similarly we may select algebraic integers ρ_s such that

$$\rho_s^{d} \not\equiv 1 \pmod{\mathfrak{p}_s}, \qquad s = 2, 3, \cdots, k,$$

provided that d is a multiple of none of the integers $\varphi(\mathfrak{p}_s)$. Now there is an algebraic integer ρ_m in Ω such that*

$$\rho_m \equiv \rho_1 \pmod{\mathfrak{p}_1}, \qquad \rho_m \equiv \rho_2 \pmod{\mathfrak{p}_2}, \qquad \cdots, \qquad \rho_m \equiv \rho_k \pmod{\mathfrak{p}_k}.$$

Then $\rho_m{}^d - 1$ is prime to each of the ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$, and is therefore prime to $\mathfrak{m}$. In (1a) put $\rho = \rho_m$, then $S \equiv 0 \pmod{\mathfrak{m}}$. Whence the following

Theorem II. *If we form an* I.H.S.F. *with the algebraic integers of a* C.S.U.R. *of an ideal modulus* $\mathfrak{m}$, *in an algebraic field* Ω, *then the resulting integer is divisible in* Ω *by* $\mathfrak{m}$, *unless the dimension of the function is divisible by one of the integers* $\varphi(\mathfrak{p}_s)$, $s = 1, 2, \cdots, k$, *where* $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$ *are the distinct ideal prime factors of* $\mathfrak{m}$.

The theorem holds also if we replace the C.S.U.R. by the complete system of incongruent residues modulo $\mathfrak{m}$.

3. Consider an I.H.S.F. formed by all the unit elements of any finite algebra A of dimension d, and let n be an integral mark of A. Let n_q be a primitive root of p_q, where m, the base of A, is

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

Let

$$n = \sum_{s=1}^{r} \left(\frac{m}{p_s^{a_s}} \right)^{\phi(p_s^{a_s})} n_s,$$

$\varphi(k)$ being the indicator of k, and put

$$d \equiv f_s \pmod{p_s - 1}, \qquad \text{where} \qquad f_s < p_s - 1.$$

Then unless one of the f's is zero, we see that $n^d - 1$ is prime to each of the integral marks $p_1, p_2, \cdots, p_r$. Consequently $n^d - 1$ is a unit in A, and from (1), $S = 0$. Whence the†

* Dirichlet-Dedekind, l. c., page 568.

† This method was used by Hensel to prove the theorem for the case of a system of integers $1, 2, \cdots, p-1$, modulo p, a prime. Cf. Kronecker, Vorlesungen über Zahlentheorie, vol. I, page 104, with reference to Hensel on page 498.

Theorem III. *An I.H.S.F. formed by all the unit elements of a finite algebra A vanishes in A except when the dimension of the function is divisible by one of the integers* $p_k - 1$, *where* $k = 1, 2, \cdots, r$, *and* $p_1, p_2, \cdots, p_r$ *are the distinct prime factors of the base of A.*

This theorem also holds if we replace the set of *unit* elements by the set of *all* the elements, as is easily seen.

4. We examine now the special finite algebra formed by the elements of a Galois field of order p^n. If θ is any element of the field which belongs to the exponent a, then the elements $\theta, \theta^2, \cdots, \theta^a$ form a group under multiplication which will be termed a sub-group in the field. By familiar methods it is possible to exhibit all the distinct elements of the field, other than zero, by the rectangular array

$$(2) \qquad \begin{array}{llll} \omega_1, & \omega_1\theta, & \cdots & \omega_1\theta^{a-1} \\ \omega_2, & \omega_2\theta, & \cdots & \omega_2\theta^{a-1} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \omega_b, & \omega_b\theta, & \cdots & \omega_b\theta^{a-1} \end{array}$$

where $ab = p^n - 1$. Consider an I.H.S.F. (which involves only ath powers) of the elements $\omega_1, \omega_2, \cdots, \omega_b$ of degree ad, say $S(\omega_1{}^a, \omega_2{}^a, \cdots, \omega_b{}^a)$. Further let i be a primitive root in the Galois field. Then

$$S((i\omega_1)^a, (i\omega_2)^a, \cdots, (i\omega_b)^a) = i^{ad}S(\omega_1{}^a, \omega_2{}^a, \cdots, \omega_b{}^a).$$

We have from (2)

$$(i\omega_k)^a = (\theta^s\omega_l)^a = \omega_l{}^a,$$

where s is some integer less than a. As k ranges over the set $1, 2, \cdots, b$, then l ranges over the same set. For otherwise we would have $(i\omega_k)^a = (i\omega_{k_1})^a$, whence $\omega_k = \theta^t\omega_{k_1}$, where $t < a$, contrary to the definition of (2). Hence in the field

$$S((i\omega_1), (i\omega_2)^a, \cdots (i\omega_b)^a) = S = i^{ad}S, \qquad (i^{ad} - 1)S = 0,$$

which gives $S = 0$, unless

$$i^{ad} - 1 = 0,$$

i. e., unless $ad \equiv 0$, (mod $p^n - 1$), since i is a primitive root in the field. This gives the

Theorem IV. *If we form a rectangular array of the elements (not zero) of a Galois field of order* p^n *with respect to a sub-group in the field of order a, then an I.H.S.F. involving only the ath powers of all the multipliers in the array is zero in the field unless the dimension d of the function is a multiple of* $(p^n - 1)/a$.

Considering the special case in which the Galois field is represented by a complete set of residues modulo p, and putting $a = 2$, we obtain the corollary: *Any I.H.S.F. formed by the system of odd incongruent residues of p, which involves only squares of these residues, is divisible by p, unless the degree of said function with respect to said squares is a multiple of $(p-1)/2$, where p is prime.*

Symmetric functions of residues of a rational modulus.

5. Examine now a complete system of residues with respect to a rational integer $m(\neq 2)$ as modulus. Consider a conjugate set in the algebra so formed and let it be represented by

$$n_1, n_2, \cdots, n_k, \qquad (n_i < m), \tag{3}$$

where k is the order of the set. Let n be any unit multiplier of the set (not unity), then the integers

$$\frac{y_a m + n_a}{n} \qquad (a = 1, 2, \cdots, k),$$

$$y_a \equiv -\frac{n_a}{m} \pmod{n} \qquad (0 \leqq y_a < n),$$

are identical with those of the set (3). For, modulo m, they reduce to n_a/n $(a = 1, 2, \cdots, k)$, which set reduces to (3) modulo m, since $1/n = n^{t-1}$ is a multiplier of the conjugate set, t being the totient of the algebra. Further, each is less than m, since y_a by hypothesis is less than n. Now form any I.H.S.F., say S, of the integers in (3) of degree i. We have

$$S(n_1, \cdots) = S\left(\frac{y_1 m + n_1}{n}, \cdots\right),$$

$$n^i S(n_1, \cdots) = S(y_1 m + n_1, \cdots). \tag{4}$$

Consider a particular term of $S(y_1 m + n_1, \cdots)$, say

$$(y_a m + a)(y_b m + b) \cdots (y_h m + h),$$

where $a, b, \cdots h$ are certain of the n's, not necessarily distinct, and i in number. This may be written

$$ab \cdots h\left(\frac{y_a}{a} m + 1\right)\left(\frac{y_b}{b} m + 1\right) \cdots \left(\frac{y_h}{h} m + 1\right),$$

and expanding in powers of m this becomes

$$abc \cdots h\left(1 + m\left[\frac{y}{ab \cdots h}\right]_1 + m^2\left[\frac{y}{ab \cdots h}\right]_2 \cdots + m^i\left[\frac{y}{ab \cdots h}\right]_i\right),$$

where

$$\left[\frac{y}{ab\cdots h}\right]_s,$$

represents the elementary symmetric function formed from

$$\frac{y_a}{a}, \frac{y_b}{b}, \cdots, \frac{y_k}{k}$$

taken s at a time.

Then by (4)

$$n^i S = \sum_{a,b\cdots h}\sum_{s=1}^{i} ab\cdots h\left(1 + m^s\left[\frac{y}{ab\cdots h}\right]_s\right),$$

where the outside summation is effected by replacing $ab\cdots h$ by all the terms of the function $S(n_1\cdots)$ in turn. This relation may be written

$$\frac{(n^i - 1)S}{m} = \sum_{ab\cdots h}\sum_{s=0}^{i-1} ab\cdots h m^s\left[\frac{y}{ab\cdots h}\right]_{s+1}. \tag{5}$$

We now proceed to set down a number of consequences of this theorem. Put $i = k$, $S = \prod_{r=1}^{k} n_r$, and divide through by S, then*

$$\frac{n^k - 1}{m} = \sum_{s=0}^{k-1} m^s\left[\frac{y}{n_1 n_2\cdots n_k}\right]_{s+1}. \tag{6}$$

Modulo m, this assumes the form, provided the conjugate set includes units only,

$$\frac{n^k - 1}{m} \equiv \sum_{r=1}^{k}\frac{y_r}{n_r} \pmod m. \tag{6a}$$

Letting $m = p$, a prime, and $k = p - 1$, with $n = 2$, and reducing the relation (6) modulo p^2, we obtain

$$q(2) \equiv 1 + \frac{1}{3} + \cdots + \frac{1}{p-2} + pP \pmod{p^2}, \tag{7}$$

where P is the elementary symmetric function of the elements

$$1, \frac{1}{3}, \cdots \frac{1}{p-2}$$

taken two at a time. Setting

$$S_a = 1 + \frac{1}{3^a} + \cdots + \frac{1}{(p-2)^a},$$

* This theorem includes as special cases most of the results of Sylvester, Comptes Rendus, vol. 52, 1861, p. 161; Mirimanoff, Crelle, vol. 115, 1895, p. 295; Baker, Proceedings of the London Mathematical Society, ser. 2, vol. IV, p. 131.

we have evidently

$$S_1^2 = S_2 + 2P.$$

By the corollary to Theorem IV we have, if $p > 3$,

$$S_2 \equiv 0 \pmod{p},$$

whence

$$S_1^2 \equiv 2P \pmod{p}.$$

From (7) we have

$$q(2) \equiv S_1 + p\frac{S_1^2}{2} \pmod{p^2} \qquad (p > 3),$$

which shows that

$$q(2) \equiv 0 \pmod{p^2}$$

if and only if

$$1 + \frac{1}{3} + \cdots + \frac{1}{p-2} \equiv 0 \pmod{p^2}.$$

Now in (5) put $S = 1^i + 2^i + \cdots + (p-1)^i$, where $m = p$. Then

$$\frac{(n^i - 1)S}{p} = \sum_{a=1}^{p-1} \sum_{s=1}^{i} a^i \binom{i}{s} \left(\frac{y_a}{a}\right)^s p^{s-1}, \tag{7a}$$

and, modulo p, this becomes, if n is any of the integers $2, 3, \cdots p-1$,

$$\frac{(n^i - 1)S}{ip} \equiv \sum_{a=1}^{p-1} y_a a^{i-1} \pmod{p}.$$

It is known that

$$1^i + 2^i + \cdots + (p-1)^i \equiv b_i p \pmod{p^2},$$

where

$$b_1 = -\tfrac{1}{2}, \qquad b_{2a+1} = 0, \qquad b_{2a} = (-1)^{a-1}B_a,$$

$B_1 = \frac{1}{6}$, $B_2 = \frac{1}{30}$, etc., being the numbers of Bernoulli, and $i < p-1$. Then

$$\frac{(n^i - 1)b_i}{i} \equiv \sum_{a=1}^{p-1} y_a a^{i-1} \pmod{p}. \tag{8}$$

6. We now introduce roots of unity and derive some new relations involving them.

Let x be an indeterminate. Then if we set

$$(x-1)F(x) = x^n - 1,$$

we have

$$(x-1)\frac{dF}{dx} + F = nx^{n-1}.$$

Letting $x = \alpha^{hm}$, where $\alpha = e^{2i\pi/n}$, and multiplying by $\alpha^{hn_a + hm}$, we may write, n being prime to m,

$$\frac{\alpha^{hn_a}}{\alpha^{hm} - 1} = \frac{\sum_{s=1}^{n-1} s\alpha^{h(ms+n_a)}}{n},$$

if h is an integer not divisible by n. We have

$$\sum_{s=1}^{n-1} s\alpha^{h(ms+n_a)} = \sum_{s_1} s_1\alpha^{h(ms_1+n_a)} + s_2,$$

where s_1 ranges over those integers less than n such that $ms_1 + n_a \not\equiv 0 \pmod{n}$, and

$$s_2 \equiv -\frac{n_a}{m} \pmod{n} \qquad (n > s_2 \geqq 0).$$

Then we obtain

$$\sum_{h=1}^{n-1}\sum_{s=1}^{n-1} s\alpha^{h(ms+n_a)} = \sum_{s_1}\sum_{h=1}^{n-1} s_1\alpha^{h(ms_1+n_a)} + (n-1)s_2.$$

The right-hand member of the above relation reduces to

$$-\frac{n(n-1)}{2} + ns_2,$$

which gives

$$\sum_{h=1}^{n-1} \frac{\alpha^{hn_a}}{\alpha^{hm}-1} + \frac{n-1}{2} = s_2 = y_a, \tag{9}$$

as previously defined. Letting $m = p$, a prime, and substituting in (7a) we obtain

$$\frac{(n^i-1)S}{p} = \sum_{a=1}^{p-1}\sum_{s=1}^{i} p^{s-1}a^{i-s}\binom{i}{s}\left(\sum_{h=1}^{n-1}\frac{\alpha^{ah}}{\alpha^{hp}-1} + \frac{n-1}{2}\right)^{s}.$$

Modulo p, this becomes ($i < p-1$),

$$\frac{(n^i-1)b_i}{i} \equiv \sum_{h=1}^{n-1}\frac{f_i(\alpha^h)}{\alpha^{hp}-1} \pmod{p},$$

where the f function has the form defined previously. Applying (9) to (6a), we have

$$\frac{n^k-1}{m} \equiv \sum_{h=1}^{n-1}\frac{f_0^{(n)}(\alpha^h)}{\alpha^{hm}-1} + \frac{n-1}{2}\sum_a \frac{1}{n_a} \pmod{m},$$

n_a ranging over all the elements of the conjugate set and

$$f_0^{(n)}(\alpha) = \sum_a n_a^{-1}\alpha^{n_a}.$$

If $n-1$ is prime to m, then Theorem I gives

$$\frac{n^k-1}{m} \equiv \sum_{h=1}^{n-1}\frac{f_0^{(n)}(\alpha^h)}{\alpha^{hm}-1} \pmod{m}. \tag{10}$$

7. If we rearrange the right-hand member of (8) by collecting like values of y_a, we may write this member as follows:

$$\sum_{c=1}^{n-1}(n-c)\left\{\left(cp-\left[\frac{(c-1)p}{n}\right]n-n\right)^{i-1}+\left(cp-\left[\frac{(c-1)p}{n}\right]n-2n\right)^{i-1}\right.$$
$$\left.+\cdots+\cdots+\left(cp-\left[\frac{cp}{n}\right]n\right)^{i-1}\right\}.$$

Reduce this expression modulo p and divide the result by $(-n)^{i-1}$. The term in the reduced form corresponding to $c = 1$ has the form

$$(n-1)\left(1^{i-1}+2^{i-1}+\cdots+\left[\frac{p}{n}\right]^{i-1}\right).$$

Similarly the term for $c = 2$ is

$$(n-2)\left\{\left(\left[\frac{p}{n}\right]+1\right)^{i-1}+\left(\left[\frac{p}{n}\right]+2\right)^{i-1}+\cdots+\left[\frac{2p}{n}\right]^{i-1}\right\}.$$

The sum of the last two expressions may be written

$$\sum_{k=1}^{[p/n]}k^{i-1}+(n-2)\sum_{k_1=1}^{[2p/n]}k_1^{i-1}.$$

In the same way the sum of the expressions for $c = 1, 2$, and 3 takes the form

$$\sum_{k=1}^{[p/n]}k^{i-1}+\sum_{k_1=1}^{[2p/n]}k_1^{i-1}+(n-3)\sum_{k_2=1}^{[3p/n]}k_2^{i-1}.$$

Proceeding in this manner we obtain finally

$$\frac{(1-n^i)b_i}{in^{i-1}}\equiv\sum_{u=1}^{n-1}\sum_{k=1}^{[up/n]}k^{i-1}\pmod p. \tag{11}$$

Put $m = p$ in (6a) and let the n's range over 1, 2, $\cdots$, $p-1$. Then applying the above process we find

$$-nq(n)\equiv\sum_{u=1}^{n-1}\sum_{k=1}^{[up/n]}\frac{1}{k}\pmod p. \tag{12}$$

Set $(n+1)$ for n in this relation and subtract; we then obtain

$$-nq(n)+(n+1)q(n+1)\equiv\Sigma\frac{1}{h}\pmod p,$$

where h ranges over the integers which satisfy

$$\frac{\beta p}{n+1}<h<\frac{\beta p}{n},$$

$\beta = 1, 2, \cdots, n$. From (11) we obtain in a similar way

$$\frac{b_i(n^{p-i}-(n+1)^{p-i}+1)}{i}\equiv\Sigma h^{i-1}\pmod p, \tag{13}$$

a relation due to Kummer* for i even.

* Abhandlungen der K. Akad. der Wiss. zu Berlin, 1857.

THE GENERALIZED LAGRANGE INDETERMINATE CONGRUENCE FOR A COMPOSITE IDEAL MODULUS.

By H. S. Vandiver.

The present paper is devoted to certain generalizations of the relation

$$(1) \qquad (x-1)(x-2)\cdots(x-(p-1)) \equiv x^{p-1}-1 \pmod{p},$$

p being a rational prime, and x an indeterminate quantity. In this connection Bauer* gave a formula involving a modulus which was a power of a rational prime. Proceeding along this line, but by a different method, we obtain extensions to cover residues with respect to any composite ideal modulus.

1. It is known† that if $\mathfrak{m}$ is an ideal in an algebraic field Ω, then the incongruent residues, modulo $\mathfrak{m}$, which are prime to $\mathfrak{m}$ (called a complete system of unit residues and denoted by C.S.U.R.) are given by

$$(3) \qquad T_1\rho_1 + T_2\rho_2 + \cdots + T_k\rho_k,$$

where T_s ranges over a C.S.U.R. modulo $\mathfrak{p}_s^{a_s}$, $\rho_s \equiv 1 \pmod{\mathfrak{p}_s^{a_s}}$, $\rho_s \equiv 0 \pmod{\mathfrak{m}/\mathfrak{p}_s^{a_s}}$, $s = 1, 2, \cdots, k$, and $\mathfrak{m} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_k^{a_k}$, the $\mathfrak{p}$'s being distinct prime ideals in Ω.

Let x be an indeterminate and consider the product $\Pi(x-U)$, where U ranges over the set (3). Now the form of (3) shows that

$$(4) \qquad \Pi(x-U) \equiv \Pi(x-T_s)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}_s^{a_s})} \pmod{\mathfrak{p}_s^{a_s}}.$$

To reduce the right-hand member we observe that a C.S.U.R. of $\mathfrak{p}_s^{a_s}$ (which for the present will be written $\mathfrak{p}^a$) is given by‡

$$(5) \qquad R_1 + \theta R_2 + \theta^2 R_3 + \cdots + \theta^{a-1}R_a,$$

where θ is an algebraic integer in Ω divisible by $\mathfrak{p}$, but not by $\mathfrak{p}^2$, and is furthermore prime to $\mathfrak{m}/\mathfrak{p}^a$, R_1 ranges over a C.S.U.R. modulo $\mathfrak{p}$, and each of the other R's runs through a complete system of residues, modulo $\mathfrak{p}$.

Reduce the right-hand member of (4) modulo $\mathfrak{p}$. By (5) it becomes

$$\Pi(x-R_1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p})},$$

modulo $\mathfrak{p}$. But we have§

* Nouvelles Annales de Mathematiques, series 4, vol. 2. See relation (10) of the present paper.

† Dirichlet-Dedekind, Zahlentheorie, 4th edition, pp. 568–9.

‡ Hilbert, Die Theorie der Algebraischen Zahlkörpers, p. 193.

§ Dirichlet-Dedekind, l. c., p. 570.

$$\Pi(x - R_1) \equiv x^{\phi(\mathfrak{p})} - 1 \pmod{\mathfrak{p}}. \tag{6}$$

Modulo $\mathfrak{p}^2$, (4) reduces to

$$\Pi(x - S)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}^2)},$$

where S ranges over a C.S.U.R., modulo $\mathfrak{p}^2$. Write

$$\Pi(x - R_1) = \psi(x, \mathfrak{p}),$$

then

$$\Pi(x - (R_1 + R_2\theta)) \equiv \prod_t \psi(x - t\theta, \mathfrak{p}) \pmod{\mathfrak{p}^2},$$

where t ranges over a complete system of residues modulo $\mathfrak{p}$. We denote by $\mathfrak{p}f(x)$ a function of x in Ω, each of whose coefficients is divisible by the ideal $\mathfrak{p}$. We can then write

$$\psi(x, \mathfrak{p}) = x^{\phi(\mathfrak{p})} - 1 + \mathfrak{p}f(x).$$

We have by Taylor's theorem

$$\psi(x - t\theta) \equiv \psi(x) - t\theta \frac{d\psi}{dx} \pmod{\mathfrak{p}^2},$$

and therefore

$$\psi(x - t\theta, \mathfrak{p}) \equiv x^{\phi(\mathfrak{p})} - \varphi(\mathfrak{p})x^{\phi(\mathfrak{p})-1}t\theta - 1 + \mathfrak{p}f(x) \pmod{\mathfrak{p}^2},$$

$$\prod_t [\psi(x - t\theta, \mathfrak{p})] \equiv (x^{\phi(\mathfrak{p})} - 1 + \mathfrak{p}f(x))^{N(\mathfrak{p})} - (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p})-1}\theta\varphi(\mathfrak{p})x^{\phi(\mathfrak{p})-1}\Sigma t \pmod{\mathfrak{p}^2},$$

where $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$.

In the relation (6) develop the left-hand member and equate coefficients of each side. We get $\Sigma t \equiv 0 \pmod{\mathfrak{p}}$, provided $N(\mathfrak{p}) \neq 2$. With this restriction on $\mathfrak{p}$ we have after further reduction

$$\prod_t [\psi(x - t\theta, \mathfrak{p})] \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^2}.$$

If $\mathfrak{m}$ is divisible by $\mathfrak{p}^n$, (4) becomes, modulo $\mathfrak{p}^n$,

$$\Pi(x - T)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}^n)},$$

where T ranges over a C.S.U.R. modulo $\mathfrak{p}^n$. Assume that for a particular n

$$\Pi(x - T) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{n-1})} \pmod{\mathfrak{p}^n}.$$

We shall then show that it necessarily follows from this assumption that

$$\Pi(x - T_1) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^n)} \pmod{\mathfrak{p}^{n+1}},$$

where T_1 ranges over a C.S.U.R. modulo $\mathfrak{p}^{n+1}$, and since the assumption holds for $n = 1$ and 2, it follows by induction that it is true for any positive integer n. If

$$\Pi(x - T) = \psi(x),$$

then

$$\Pi(x - T_1) = \prod_t \psi(x - t\theta^n),$$

where t ranges over a complete set of incongruent residues modulo $\mathfrak{p}$.

Let

$$\psi(x) = (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{n-1})} + \mathfrak{p}^n f(x),$$

where $\mathfrak{p}^n f(x)$ denotes a function of x in Ω, each of whose coefficients are divisible by $\mathfrak{p}^n$. Then for a fixed t

$$\psi(x - t\theta^n) = [(x - t\theta^n)^{\phi(\mathfrak{p})} - 1]^{N(\mathfrak{p}^{n-1})} + \mathfrak{p}^n f(x - t\theta^n)$$
$$\equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{n-1})} + \mathfrak{p}^n f(x) \pmod{\mathfrak{p}^{n+1}},$$

and

$$\prod_t \psi(x - t\theta^n) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^n)} \pmod{\mathfrak{p}^{n+1}},$$

the desired result.

Using (4) we then have

$$\Pi(x - U) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{a-1}) \times \phi(\mathfrak{m})/\phi(\mathfrak{p}^a)} \pmod{\mathfrak{p}^a}$$
$$\equiv (x^{\phi(\mathfrak{p})} - 1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p})} \pmod{\mathfrak{p}^a}.$$

We may then write

$$\Pi(x - U) \equiv \sum_{s=1}^{k} \rho_s (x^{\phi(\mathfrak{p}_s)} - 1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}_s)} \pmod{\mathfrak{m}}, \tag{8}$$

where

$$\rho_s \equiv 1 \pmod{\mathfrak{p}_s^{a_s}}, \qquad \rho_s \equiv 0 \pmod{\mathfrak{m}/\mathfrak{p}_s^{a_s}}.$$

2. Now consider the case where $N(\mathfrak{p}) = 2$, which was excluded from the previous discussion. Suppose 2 is divisible by the prime ideal $\mathfrak{p}$, but not by $\mathfrak{p}^2$. Then we may take $2 = \theta$. Write

$$\Pi(x - T) = \psi(x, \mathfrak{p}^n),$$

where T ranges over a C.S.U.R. modulo $\mathfrak{p}^n$. Then

$$\psi(x, \mathfrak{p}^2) \equiv (x - 1)(x - (1 + 2)) \pmod 4$$
$$\equiv (x^2 - 1) \pmod 4,$$
$$\psi(x, \mathfrak{p}^3) \equiv \psi(x, \mathfrak{p}^2)\psi(x - 4, \mathfrak{p}^2) \pmod 8$$
$$\equiv (x^2 - 1)^2 \pmod 8,$$

and in general

$$\psi(x, \mathfrak{p}^n) \equiv (x^2 - 1)^{\phi(\mathfrak{p}^n)/2} \pmod{\mathfrak{p}^n}, \tag{9}$$

where $n > 1$.

Suppose that 2 is divisible by $\mathfrak{p}^2$. Then proceeding as above, we find, if θ is an algebraic integer in Ω divisible by $\mathfrak{p}$, but not by $\mathfrak{p}^2$,

$$\psi(x, \mathfrak{p}^2) = (x - 1)^2 - \theta(x - 1) + \mathfrak{p}^2 f(x),$$

and using

$$\psi(x, \mathfrak{p}^3) \equiv \psi(x, \mathfrak{p}^2)\psi(x - \theta^2, \mathfrak{p}^2) \pmod{\mathfrak{p}^3},$$

we get

$$\psi(x, \mathfrak{p}^3) \equiv [(x - 1)^2 - \theta(x - 1)]^2 \pmod{\mathfrak{p}^3}.$$

Similarly,

$$\psi(x, \mathfrak{p}^4) \equiv (x^2 - 1)^4 \pmod{\mathfrak{p}^4},$$

and in general we get (9) for $n > 3$.

3. By using methods similar to those employed above we can show that

$$\Pi(x - U') \equiv \sum_{s=1}^{k} \rho_s (x^{N(\mathfrak{p}_s)} - x)^{N(\mathfrak{m})/N(\mathfrak{p}_s)} \pmod{\mathfrak{m}}, \tag{8'}$$

where U' ranges over all the incongruent residues modulo $\mathfrak{m}$, and $N(\mathfrak{p}_s) \neq 2$.

Let

$$\omega(x, \mathfrak{p}^n) = \Pi(x - T'),$$

where T' ranges over all the incongruent residues modulo $\mathfrak{p}^n$, when $N(\mathfrak{p}) = 2$.

We have, if 2 is divisible by $\mathfrak{p}$, but not by $\mathfrak{p}^2$,

$$\begin{aligned} \omega(x, \mathfrak{p}^2) &\equiv x(x-1)(x-2)(x-(1+2)) \pmod{\mathfrak{p}^2} \\ &\equiv (x^2-1)(x^2-2x) \pmod{\mathfrak{p}^2}, \\ \omega(x, \mathfrak{p}^3) &\equiv \omega(x, \mathfrak{p}^2)\omega(x-4, \mathfrak{p}^2) \pmod{\mathfrak{p}^3} \\ &\equiv (x^2-1)^2(x^2-2x)^2 \pmod{\mathfrak{p}^3}, \end{aligned}$$

and in general

$$\omega(x, \mathfrak{p}^n) \equiv [(x^2-1)(x^2-2x)]^{\frac{N(\mathfrak{p}^n)}{4}} \pmod{\mathfrak{p}^n}, \tag{9'}$$

where $n > 1$. Similarly, if 2 is divisible by $\mathfrak{p}^2$, we obtain (9') for $n > 3$.

By means of (8), (8'), (9), (9') we can express in a simplified form any elementary symmetric function formed by all the incongruent unit residues modulo $\mathfrak{m}$, or any function of the same type formed by all the incongruent residues modulo $\mathfrak{m}$, where $\mathfrak{m}$ is *any* ideal in Ω. In particular, putting $x = 0$ in (8) we have

Theorem I. *The product formed by the set of all incongruent unit residues modulo* $\mathfrak{m}$, *an ideal in an algebraic field* Ω, *prime to 2, is congruent to minus unity or unity modulo* $\mathfrak{m}$, *according as* $\mathfrak{m}$ *possesses one or more than one distinct ideal prime factor.*

This is evidently a generalization of Wilson's theorem. The results of (8) and (8') may be expressed by

Theorem II. *If* $\mathfrak{m}$ *is an ideal in an algebraic field* Ω, *and*

$$\mathfrak{m} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_k^{a_k} \qquad (N(\mathfrak{p}_s) \neq 2),$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$ *are distinct prime ideals in* Ω, *then*

$$\Pi(x - U) \equiv \sum_{s=1}^{k} \rho_s (x^{\phi(\mathfrak{p}_s)} - 1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}_s)} \pmod{\mathfrak{m}},$$

where U *ranges over all incongruent unit residues modulo* $\mathfrak{m}$, *and*

$$\Pi(x - U') \equiv \sum_{s=1}^{k} \rho_s (x^{N(\mathfrak{p}_s)} - x)^{N(\mathfrak{m})/N(\mathfrak{p}_s)} \pmod{\mathfrak{m}},$$

where U' ranges over all the incongruent residues modulo $\mathfrak{m}$. The ρ's are defined by

$$\rho_s \equiv 1 \pmod{\mathfrak{p}_s^{a_s}}, \qquad \rho_s \equiv 0 \left(\mod \frac{\mathfrak{m}}{\mathfrak{p}_s^{a_s}}\right),$$

$s = 1, 2, \cdots, k$. Further, x is an indeterminate, $\varphi(k)$ is the indicator of k, and $N(k)$ denotes the norm.

If we suppose that Ω is the field of rational numbers, then the relations (8) and (8′) may be written (if the modulus $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where the p's are prime)

$$\Pi(x - U) \equiv \sum_{s=1}^{k} (m/p_s^{a_s})^{\phi(p_s^{a_s})} (x^{\phi(p_s)} - 1)^{\phi(m)/\phi(p_s)} \pmod{m}, \tag{10}$$

$$\Pi(x - U') \equiv \sum_{s=1}^{k} (m/p_s^{a_s})^{\phi(p_s^{a_s})} (x^{p_s} - x)^{m/p_s} \pmod{m}. \tag{11}$$

For the modulus $m = p^a$, the first relation was given by Bauer, as before noted.

4. Relations (8) and (8′) may be derived in a way a bit different from that previously used, by extending a method employed by Bauer in the article cited. Retaining the former notation, consider

$$\prod_{R_2} (x - (r + R_2\theta)) \pmod{\mathfrak{p}^2},$$

where r is fixed. This reduces to

$$(x - r)^{N(\mathfrak{p})} - (x - r)^{N(\mathfrak{p})-1} \Sigma R_2 \theta \pmod{\mathfrak{p}^2},$$

and (6) gives $\Sigma R_2 \equiv 0 \pmod{\mathfrak{p}}$, unless $\phi(\mathfrak{p}) = 1$, or $N(\mathfrak{p}) = 2$. With this exception the above expression becomes

$$(x - r)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^2},$$

and by (6)

$$\prod_{r} (x - r)^{N(\mathfrak{p})} = (x^{\phi(\mathfrak{p})} - 1 + \mathfrak{p} f(x))^{N(\mathfrak{p})},$$

or

$$\Pi (x - (R_1 + R_2\theta)) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^2}.$$

Using a method similar to the above we derive (8) by induction after employing (4). The relation (8′) follows in like manner.

ON THE CONGRUENCE $cx^\lambda + 1 \equiv dy^\lambda$ IN A GALOIS FIELD.*

By Howard H. Mitchell.

Introduction.

1. In another paper† the author has considered the relation between a certain cyclotomic function and the congruences

$$cx^\lambda + 1 \equiv dy^\lambda$$

in a Galois field of order q^t, where $q^t = \lambda\nu + 1$, and c, d are any marks in the field different from 0. If c and d are expressed as powers of a primitive root in the field, and

$$\text{ind } c \equiv i, \qquad \text{ind } d \equiv j, \qquad \text{mod } \lambda,$$

we shall denote the number of solutions of the congruence by m_i^j. The object of the present paper is to obtain certain results concerning the numbers m_i^j.

For the case where q is a prime of the form $\lambda\nu + 1$ and $t = 1$ the problem has been considered by a number of other authors. Gauss showed that for $\lambda = 3$ the determination of the numbers m_i^j could be accomplished by means of the representation of $4q$ by the form $A^2 + 27B^2$, and for $\lambda = 4$ by means of the representation of q by the form $A^2 + B^2$. In a recent paper Dickson obtained a lower limit for the number of solutions when λ is prime and $c \equiv d \equiv 1$, mod q, and thereby showed that solutions exist for every q exceeding a certain limit in terms of λ. Hurwitz later extended this result by obtaining both upper and lower limits for any pair of residues c, d.‡

The author obtains three results in the present paper. By means of certain properties of congruences it is first shown that the values of the numbers m_i^j are completely determined by means of a particular set of equations. By means of this result the exact values of these numbers are found for a Galois field of order q^{2t}, provided t has a divisor t_1 such that $q^{t_1} \equiv -1$, mod λ. Finally it is shown that, if $q^t \equiv 1$, mod λ, the numbers

* Presented to the American Mathematical Society, Dec. 28, 1915.

† Transactions of the American Mathematical Society, vol. 17 (1916), pp. 165–177.

‡ Gauss, Disquisitiones Arithmeticæ, § 358; Theoria Residuorum Biquadraticorum, §§ 15–20; Lebesgue, Journal de Mathematiques, vol. 2 (1837), pp. 253–292; Carey, Quarterly Journal of Mathematics, vol. 26 (1893), pp. 322–371; Dickson, Journal für Mathematik, vol. 135 (1909), pp. 181–188; Hurwitz, ibid., vol. 136 (1909), pp. 272–292; Cornacchia, Giornale di mathematische di Battaglini, vol. 47 (1909), pp. 219–268.

m_i^j for a field of order q^{st} may be expressed in terms of the similar numbers for a field of order q^t.

A lemma concerning congruences.

2. In what follows we shall denote by the symbol $dv(a, b, c, \cdots)$ the greatest common divisor of the integers $a, b, c, \cdots$. We consider a, b to be any pair of residues, mod λ, such that $dv(\lambda, a, b) = 1$. We shall also regard ka, kb as the same as a, b provided k is prime to λ. The total number of such pairs is equal to

$$\frac{\varphi_2(\lambda)}{\varphi(\lambda)},$$

where

$$\varphi(\lambda) = \lambda\Pi\left(1 - \frac{1}{\pi_i}\right), \qquad \varphi_2(\lambda) = \lambda^2\Pi\left(1 - \frac{1}{\pi_i^2}\right)$$

are the φ-functions of the first and second order respectively,* and where the products are to be taken over the different primes π_i contained in λ.

We shall need to determine for how many such pairs a, b

$$dv(\lambda, ax + by) = \frac{\lambda}{\tau}, \tag{1}$$

where x, y are any integers, and τ is a divisor of λ. If we write

$$dv(\lambda, x, y) = \sigma, \tag{2}$$

it is evident that there will be no such pairs if λ/τ is not divisible by σ.

We shall prove

LEMMA 1. *The number of pairs of residues a, b, mod λ, such that*

(*a*) $dv(\lambda, a, b) = 1$,

(*b*) *ka, kb is regarded as the same as a, b if k is prime to λ,*

(*c*) *condition* (1) *is satisfied,*

(*d*) *λ/τ is divisible by σ, is equal to*

$$\sigma\Pi\left(1 + \frac{1}{\pi_i}\right) \times \tau\Pi\left(1 - \frac{1}{\pi_j}\right),$$

where the first product is to be taken over all the different primes π_i that are contained in σ to as high a power as in λ, and the second product over all the different primes π_j that are contained in τ, but not to as high a power as in λ/σ.

We put

$$dv\left(\frac{\lambda}{\tau}, x\right) = \beta\sigma, \qquad dv\left(\frac{\lambda}{\tau}, y\right) = \alpha\sigma,$$

so that α and β have no common factor, and write also

$$\lambda = \alpha\beta\rho\sigma\tau.$$

* Cahen, Elements de la Theorie des Nombres, 1900, p. 36.

In order that

$$ax + by \equiv 0, \qquad \text{mod } \frac{\lambda}{\tau},$$

a must be divisible by α, and b by β, so that we have

$$\frac{a}{\alpha}x' + \frac{b}{\beta}y' \equiv 0, \qquad \text{mod } \rho, \tag{3}$$

where $x' = x/\beta\sigma$, and $y' = y/\alpha\sigma$, are each prime to ρ.

In order that $dv(\rho, a, b) = 1$, a/α and b/β must each be prime to ρ, and for each value of a/α, prime to ρ, there will be exactly one value of b/β, mod ρ, for which the congruence is satisfied. We shall at first consider ka, kb as different from a, b for $k \not\equiv 1$, mod λ, and hence we may consider the pairs a, b for which the congruence (3) is satisfied, and for which $dv(\rho, a, b) = 1$, to be divided into $\varphi(\rho)$ sets according to the residues of a/α, b/β, mod ρ.

The pairs a, b for which a/α, b/β have particular residues, mod ρ, may be represented by the equations

$$\frac{a}{\alpha} = \frac{a_0}{\alpha} + h\rho, \qquad \frac{b}{\beta} = \frac{b_0}{\beta} + l\rho,$$

where a_0, b_0 represent a particular pair such that a_0/α, b_0/β are each less than ρ, and $h = 0, 1, 2, \cdots, \beta\sigma\tau - 1$; $l = 0, 1, 2, \cdots, \alpha\sigma\tau - 1$.

In order that $dv(\alpha\beta, a, b) = 1$, we must choose h so that a is prime to β, and l so that b is prime to α. Since a/α is prime to ρ for all values of h, we merely need to choose h so that a/α is prime to $\bar{\beta}$, where $\bar{\beta}$ represents the product of all the factors contained in β that are prime to ρ. As h assumes the values of a complete residue system, mod $\bar{\beta}$, the same is true of $h\rho$, and hence also of a/α. There are consequently $\varphi(\bar{\beta})$ values of h, mod $\bar{\beta}$, and hence $\varphi(\bar{\beta})\beta/\bar{\beta}$ values of h, mod β, for which a/α is prime to $\bar{\beta}$.

Similarly, if $\bar{\alpha}$ represents the product of all the factors contained in α that are prime to ρ, there are $\varphi(\bar{\alpha})\alpha/\bar{\alpha}$ values of l, mod α, for which b/β is prime to $\bar{\alpha}$. Hence the pairs a, b for which the congruence (3) is satisfied, and such that $dv(\alpha\beta\rho, a, b) = 1$, may be divided into

$$\varphi(\rho) \cdot \varphi(\bar{\beta}) \frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha}) \frac{\alpha}{\bar{\alpha}}$$

sets according to the residues of a/α, mod $\beta\rho$, and b/β, mod $\alpha\rho$.

The pairs a, b for which a/α has a particular residue, mod $\beta\rho$, and b/β a particular residue, mod $\alpha\rho$, may be represented by the equations

$$\frac{a}{\alpha} = \frac{a_1}{\alpha} + h'\beta\rho, \qquad \frac{b}{\beta} = \frac{b_1}{\beta} + l'\alpha\rho,$$

where a_1, b_1 represent a particular pair such that a_1/α and b_1/β are less than $\beta\rho$ and $\alpha\rho$ respectively, and h', $l' = 0, 1, 2, \cdots, \sigma\tau - 1$.

In order that condition (1) shall hold we must have

$$(4) \quad \frac{a}{\alpha}x' + \frac{b}{\beta}y' \equiv \left(\frac{a_1}{\alpha}x' + \frac{b_1}{\beta}y'\right) + (h'\beta x' + l'\alpha y')\rho \equiv \mu\rho, \qquad \text{mod } \tau\rho,$$

where μ is prime to τ. Since

$$\beta x' = \frac{x}{\sigma}, \qquad \alpha y' = \frac{y}{\sigma}, \qquad dv\left(\frac{\lambda}{\sigma}, \frac{x}{\sigma}, \frac{y}{\sigma}\right) = 1,$$

we have

$$dv(\tau, \beta x', \alpha y') = 1.$$

Hence by a proper choice of h', l', mod τ, we may make $h'\beta x' + l'\alpha y'$ assume any residue, mod τ. Moreover, there are exactly as many pairs h', l', mod τ, for which this expression assumes the residue 0, mod τ, as pairs for which it assumes any other residue, and hence the expression assumes any desired residue for exactly τ of the τ^2 pairs. Since there are $\varphi(\tau)$ residues μ, prime to τ, we conclude that there are $\varphi(\tau)\tau$ pairs h', l', mod τ, for which the condition (4) is satisfied.

Moreover, when condition (4) is satisfied, we have also $dv(\tau, a, b) = 1$. For all the pairs a, b that we are now considering satisfy the condition, $dv(\alpha\beta\rho, a, b) = 1$. Hence $dv(\tau, a, b)$ must be prime to $\alpha\beta\rho$. It then follows from condition (4) that it must have the value 1.

We conclude that the pairs a, b for which (4) is satisfied, and such that $dv(\alpha\beta\rho\tau, a, b) = 1$, may be divided into

$$\varphi(\rho) \cdot \varphi(\bar{\beta})\frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha})\frac{\alpha}{\bar{\alpha}} \cdot \varphi(\tau)\tau$$

sets according to the residues of a/α, mod $\beta\rho\tau$, and b/β, mod $\alpha\rho\tau$.

The pairs a, b for which a/α has a particular residue, mod $\beta\rho\tau$, and b/β a particular residue, mod $\alpha\rho\tau$, may be represented by the equations

$$\frac{a}{\alpha} = \frac{a_2}{\alpha} + h''\beta\rho\tau, \qquad \frac{b}{\beta} = \frac{b_2}{\beta} + l''\alpha\rho\tau,$$

where a_2, b_2 represent a particular pair such that a_2/α and b_2/β are less than $\beta\rho\tau$ and $\alpha\rho\tau$ respectively, and where h'', $l'' = 0, 1, 2, \cdots, \sigma - 1$. For all these the condition (4) is satisfied, and $dv(\alpha\beta\rho\tau, a, b) = 1$. It remains only to impose the condition $dv(\sigma, a, b) = 1$. This will be true provided $dv(\bar{\sigma}, a, b) = 1$, where $\bar{\sigma}$ represents the product of all the factors contained in σ that are prime to $\alpha\beta\rho\tau$.

As h'', l'' assume independently the values of complete residue systems, mod $\bar{\sigma}$, the same is true of $h''\beta\rho\tau$ and $l''\alpha\rho\tau$, and hence also of a/α and

b/β. The number of pairs of residues, mod $\bar{\sigma}$, whose greatest common divisor is prime to $\bar{\sigma}$, is by definition $\varphi_2(\bar{\sigma})$.* Since there are $\sigma/\bar{\sigma}$ values of h'' for which a/α assumes a particular residue, mod $\bar{\sigma}$, and $\sigma/\bar{\sigma}$ values of l'' for which b/β assumes a particular residue, mod $\bar{\sigma}$, there are $\varphi_2(\bar{\sigma})\sigma^2/\bar{\sigma}^2$ pairs h'', l'' for which $dv(\bar{\sigma}, a, b) = 1$.

We conclude therefore that there are

$$\varphi(\rho) \cdot \varphi(\bar{\beta}) \frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha}) \frac{\alpha}{\bar{\alpha}} \cdot \varphi(\tau)\tau \cdot \varphi_2(\bar{\sigma}) \frac{\sigma^2}{\bar{\sigma}^2}$$

pairs a, b for which $dv(\lambda, a, b) = 1$, for which condition (4) is satisfied, and such that ka, kb is regarded as different from a, b if $k \equiv 1$, mod λ. Since we wish finally to regard such pairs as the same, we must divide the above number by $\varphi(\lambda)$. This may be written in the form

$$\varphi(\lambda) = \varphi(\rho) \cdot \varphi(\bar{\beta}) \frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha}) \frac{\alpha}{\bar{\alpha}} \cdot \varphi(\bar{\tau}) \frac{\tau}{\bar{\tau}} \cdot \varphi(\bar{\sigma}) \frac{\sigma}{\bar{\sigma}},$$

where $\bar{\tau}$ represents the product of all the factors contained in τ that are prime to $\alpha\beta\rho$. Hence the desired result is

$$\frac{\bar{\tau}}{\varphi(\bar{\tau})} \cdot \frac{\sigma}{\bar{\sigma}} \frac{\varphi_2(\bar{\sigma})}{\varphi(\bar{\sigma})}.$$

We may write

$$\varphi(\tau) = \tau\Pi\left(1 - \frac{1}{\pi_k}\right),$$

$$\varphi(\bar{\tau}) = \bar{\tau}\Pi\left(1 - \frac{1}{\bar{\pi}_k}\right),$$

$$\varphi_2(\bar{\sigma}) = \bar{\sigma}^2\Pi\left(1 - \frac{1}{\pi_i^2}\right),$$

$$\varphi(\bar{\sigma}) = \bar{\sigma}\Pi\left(1 - \frac{1}{\pi_i}\right),$$

where the first product is to be taken over all the different primes π_k contained in τ, the second over the different primes $\bar{\pi}_k$ contained in $\bar{\tau}$ (i. e., in τ, but not in $\alpha\beta\rho$), and the last two products over the different primes π_i contained in $\bar{\sigma}$ (i. e., in σ, but not in $\alpha\beta\rho\tau$). When we substitute these expressions in our result and make the possible cancellations, we obtain finally

$$\tau\Pi\left(1 - \frac{1}{\pi_j}\right) \times \sigma\Pi\left(1 + \frac{1}{\pi_i}\right),$$

where the first product is to be taken over all the different primes π_j con-

* Cahen, l. c.

tained in τ, but not to as high a power as in λ/σ, and the second over the different primes π_i contained in σ to as high a power as in λ. We have thus established Lemma 1.

A system of equations which determine the numbers m_i^j.

3. We now consider the congruence

$$cx^\lambda + 1 \equiv dy^\lambda$$

in a Galois field of order $q^t = \lambda\nu + 1$ and denote the number of its solutions by m_i^j, where c and d are supposed expressed as powers of a primitive root in the field, and ind $c \equiv i$, ind $d \equiv j$, mod λ. Two solutions for which x^λ, y^λ have the same values will be considered as the same. The residue, ind (-1), mod λ, will be denoted by ϵ. This has the value 0 unless q and ν are both odd, in which case it is $\lambda/2$.

The following relations between the numbers m_i^j are well known:

$$m_i^j = m_{j+\epsilon}^{i+\epsilon} = m_{-j+\epsilon}^{i-j} = m_{i-j+\epsilon}^{-j} = m_{-i}^{j-i} = m_{j-i+\epsilon}^{-i+\epsilon}; \tag{1}$$

$$\sum_i m_i^0 = \nu - 1; \qquad \sum_i m_i^j = \nu; \tag{2}$$

where $i = 0, 1, 2, \cdots, \lambda - 1$; $j \not\equiv 0$, mod λ.

Another relation may be easily proved. For from the given congruence we have

$$c^q x^{q\lambda} + 1 \equiv d^q y^{q\lambda}.$$

Conversely by raising this congruence to the power q^{t-1}, we conclude that if it is satisfied the given congruence must be. Hence we have $m_{qi}^{qj} = m_i^j$, or more generally

$$m_{i'}^{j'} = m_i^j, \tag{3}$$

provided for some integer k, $j' \equiv q^k j$. $i' \equiv q^k i$, mod λ.

We define $M_{a,b,c}$ to be sum of the λ numbers m_i^j for which the congruence

$$aj + bi \equiv c, \qquad \text{mod } \lambda, \tag{4}$$

is satisfied, where we suppose that $dv(\lambda, a, b) = 1$. The number of distinct congruences of this type is equal to

$$\frac{\varphi_2(\lambda)}{\varphi(\lambda)} \cdot \lambda = \psi(\lambda) \cdot \lambda.$$

Theorem 1. *The λ^2 quantities m_i^j are completely determined by the set of $\lambda\psi(\lambda)$ equations*

$$\Sigma m_i^j = M_{a,b,c}, \tag{5}$$

where the values of the numbers $M_{a,b,c}$ are supposed known, and i, j assume as values the λ pairs of residues for which the congruence (4) *is satisfied.*

We divide the equations (5) into sets with respect to a particular one of the numbers m_i^j, say $m_{i_0}^{j_0}$, as follows. We designate as an equation E_τ any one of the equations (5) for which

$$dv(\lambda, aj_0 + bi_0 - c) = \frac{\lambda}{\tau}. \tag{6}$$

Hence $m_{i_0}^{j_0}$ will appear in each of the $\psi(\lambda)$ equations E_1, and in none of the others.

We inquire how many times any other m_i^j will appear in the set E_τ. For any equation in this set we have

$$dv[\lambda, a(j - j_0) + b(i - i_0)] = \frac{\lambda}{\tau},$$

and hence if we put

$$\sigma = dv(\lambda, i - i_0, j - j_0), \tag{7}$$

it follows that λ/τ is divisible by σ.

By Lemma 1 the number of times m_i^j appears in the set E_τ is equal to

$$\sigma\Pi\left(1 + \frac{1}{\pi_i}\right) \times \tau\Pi\left(1 - \frac{1}{\pi_j}\right), \tag{8}$$

where the products are to be taken respectively over the different primes π_i contained in σ to as high a power as in λ, and the different primes π_j contained in τ, but not to as high a power as in λ/σ. We shall denote the second factor of the product (8) by $f(\tau)$, since in the discussion λ and σ will be supposed fixed.

We now multiply each of the equations E_τ by $(-1)^r/\chi(\tau)$, where $\chi(1) = 1$, whereas if

$$\tau = \pi_1^{\tau_1}\pi_2^{\tau_2}, \cdots \pi_r^{\tau_r},$$

$$\chi(\tau) = \pi_1^{2\tau_1 - 1}\pi_2^{2\tau_2 - 1} \cdots \pi_r^{2\tau_r - 1}. \tag{9}$$

We then form the sum of all the equations thus obtained, τ being allowed to range over all the divisors of λ, and shall show that the result is

$$\psi(\lambda)m_{i_0}^{j_0} = \Sigma \frac{(-1)^r}{\chi(\tau)} M_{a,b,c}, \tag{10}$$

where the sum is taken over all the $\lambda\psi(\lambda)$ numbers $M_{a,b,c}$, and τ is defined by (6).

Since $m_{i_0}^{j_0}$ appears in each of the equations E_1, and in none of the others, the coefficient of $m_{i_0}^{j_0}$ in this sum is $\psi(\lambda)$. Another m_i^j cannot appear in

any equations E_τ for which λ/τ is not divisible by σ, where σ is defined by (7). The coefficient of m_i^j in (10) is equal to the first factor of the product (8) multiplied by

$$\Sigma(-1)^r \frac{f(\tau)}{\chi(\tau)}, \tag{11}$$

where the sum is to be taken over all the divisors τ of λ/σ, and r denotes the number of different prime factors contained in τ.

We shall show that the sum (11) vanishes. We observe that if τ be expressed as in (9),

$$f(\tau) = f(\pi_1^{e_1}) f(\pi_2^{e_2}) \cdots f(\pi_r^{e_r}).$$

Also if the highest power of a prime π contained in λ/σ be π^h,

$$\sum_{e=1}^{h} \frac{f(\pi^e)}{\pi^{2e-1}} = \frac{\pi - 1}{\pi} + \frac{\pi^2 - \pi}{\pi^3} + \cdots + \frac{\pi^{h-1} - \pi^{h-2}}{\pi^{2h-3}} + \frac{\pi^h}{\pi^{2h-1}} = 1.$$

Hence if

$$\lambda/\sigma = \pi_1^{h_1} \pi_2^{h_2} \cdots \pi_s^{h_s},$$

then

$$\sum_{e_i=1}^{h_i} \frac{f(\pi_1^{e_1} \pi_2^{e_2} \cdots \pi_r^{e_r})}{\pi_1^{2e_1-1} \pi_2^{2e_2-1} \cdots \pi_r^{2e_r-1}} = 1.$$

Hence the sum (11) may be written

$$\sum_{r=0}^{s} (-1)^r \binom{s}{r} = 0.$$

Consequently equation (10) is true and equations (5) therefore completely determine the quantities m_i^j.

Determination of the numbers m_i^j for a special type of field.

4. We shall now obtain exact expressions for the numbers m_i^j for a field of order q^{2t}, provided there exists an exponent t_1, where $t = st_1$, such that $q^{t_1} \equiv -1$, mod λ. We have in this case by a result established in the author's other paper*

$$\sum_{i,j} m_i^j \alpha^{aj+bi} = (-1)^{s-1} q^t, \tag{1}$$

where α is a primitive λth root of unity, a, b are any integers such that $a \not\equiv 0$, $b \not\equiv 0$, $a + b \not\equiv 0$, mod λ, and i, j range independently over the residues 0, 1, 2, $\cdots$, $\lambda - 1$.

For a field of this sort, if q is odd, ν must be even, and hence $\epsilon \equiv \text{ind}\,(-1) \equiv 0$, mod λ. We therefore find from equations (1) and (2), § 3, that the value of the left-hand side of equation (1) is -1 in case exactly

* L. c., p. 177.

one of the three congruences

$$a \equiv 0, \qquad b \equiv 0, \qquad a + b \equiv 0, \qquad \text{mod } \lambda,$$

is satisfied, and $q^{2t} - 2$ in case all three are satisfied.

If, as previously, we assume that $dv(\lambda, a, b) = 1$, we may write

$$\sum_c M_{a,b,c}\alpha^{kc} = (-1)^{s-1}q^t, \ -1, \ q^{2t} - 2, \tag{2}$$

according as none of the congruences

$$ka \equiv 0, \qquad kb \equiv 0, \qquad k(a + b) \equiv 0, \qquad \text{mod } \lambda, \tag{3}$$

is satisfied, one of them is satisfied, or all three are satisfied, where $M_{a,b,c}$ has the meaning defined in § 3, and $c = 0, 1, 2, \cdots, \lambda - 1$.

We write

$$dv(\lambda, a) = a', \qquad dv(\lambda, b) = b', \qquad dv(\lambda, a + b) = d'. \tag{4}$$

If we multiply each of the equations (2) by α^{-kc}, where c is fixed, and then form the sum for $k = 0, 1, 2, \cdots, \lambda - 1$, we obtain

$$M_{a,b,c} = \frac{1}{\lambda}\left[q^{2t} - 2 - \sum_k \alpha^{-kc} + (-1)^{s-1}q^t \sum_k \alpha^{-kc}\right], \tag{5}$$

where in the first of the two sums on the right k assumes the $a' + b' + d' - 3$ values for which exactly one of the congruences (3) is satisfied, and in the second sum the $\lambda - a' - b' - d' + 2$ values for which none of them are satisfied.

The sum of the expressions α^{-kc} for the $a' - 1$ values of k other than 0 for which the first of the congruences (3) is satisfied is $a' - 1$ or -1 according as c is or is not divisible by a', and similarly for the other two sets of the same sort. The sum of all the $\lambda - 1$ expressions α^{-kc} ($k = 1, 2, \cdots, \lambda - 1$) is $\lambda - 1$ or -1 according as $c \equiv 0, \not\equiv 0, \text{mod } \lambda$. Hence the values of $M_{a,b,c}$ in the various cases are:

$$M_{a,b,0} = \frac{1}{\lambda}[q^{2t} + (\lambda + 2 - a' - b' - d')(-1)^{s-1}q^t - (a' + b' + d') + 1]; \tag{5a}$$

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + (2 - a' - b' - d')(-1)^{s-1}q^t - (a' + b' + d') + 1], \tag{5b}$$

for $c \not\equiv 0, \text{mod } \lambda$, $c \equiv 0, \text{mod } a', b', d'$;

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + (2 - a' - b')(-1)^{s-1}q^t - (a' + b') + 1], \tag{5c}$$

for $c \not\equiv 0, \text{mod } d', c \equiv 0, \text{mod } a', b'$;

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + (2 - a')(-1)^{s-1}q^t - a' + 1], \tag{5d}$$

for $c \not\equiv 0$, mod b', d', $c \equiv 0$, mod a';

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + 2(-1)^{s-1}q^t + 1], \tag{5e}$$

for $c \not\equiv 0$, mod a', b', d'. Any other case is essentially equivalent to one of these.

We first suppose that λ is prime. In this case a', b', d' all have the value 1, or one has the value λ and the other two the value 1, according as none of the congruences

$$a \equiv 0, \qquad b \equiv 0, \qquad a + b \equiv 0, \mod \lambda, \tag{6}$$

is satisfied, or one of them is satisfied. Hence if $c \equiv 0$, mod λ, we have in these two cases

$$M_{a,b,0} = \frac{1}{\lambda}[q^{2t} + (\lambda - 1)(-1)^{s-1}q^t - 2], \tag{7}$$

$$M_{a,b,0} = \frac{1}{\lambda}[q^{2t} - \lambda - 1], \tag{7'}$$

respectively, whereas if $c \not\equiv 0$, mod λ, we have correspondingly

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} - (-1)^{s-1}q^t - 2], \tag{8}$$

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} - 1]. \tag{8'}$$

There are for λ prime $\lambda^2 + \lambda$ equations of the type (5), § 3, and a particular $m_{i_0}{}^{j_0}$ appears in $\lambda + 1$ of these, i. e., the equations E_1 of § 3. For any other $m_i{}^j$ the value of σ [see (6), § 3] is 1, so that it appears exactly once in the equations E_1. The sum of the left-hand members of these equations E_1 is therefore [by use of equations (2), § 3] equal to

$$\lambda m_{i_0}{}^{j_0} + q^{2t} - 2. \tag{9}$$

For i_0, $j_0 \equiv 0$, 0, mod λ, three of the right-hand members of the $\lambda + 1$ equations E_1 have the value given by (7') and the rest the value given by (7). If exactly one of the three congruences

$$i_0 \equiv 0, \qquad j_0 \equiv 0, \qquad i_0 \equiv j_0, \mod \lambda,$$

is satisfied, one of the right-hand members has the value given by (7'), two the value given by (8'), and the rest the value given by (8). If none of those congruences are satisfied, one has the value given by (7), three the value given by (8'), and the rest the value given by (8).

If, therefore, we add these values and equate the results to (9), we obtain

in the three cases

$$m_0{}^0 = \frac{1}{\lambda^2}[q^{2t} + (\lambda - 1)(\lambda - 2)(-1)^{s-1}q^t - 3\lambda + 1],$$

$$(10) \qquad m_i{}^0 = m_0{}^i = m_{-i}^{-i} = \frac{1}{\lambda^2}[q^{2t} - (\lambda - 2)(-1)^{s-1}q^t - \lambda + 1],$$

$$m_i{}^j = \frac{1}{\lambda^2}[q^{2t} + 2(-1)^{s-1}q^t + 1],$$

where $i \not\equiv 0$, $j \not\equiv 0$, $i \not\equiv j$, mod λ.

Dickson* and Hurwitz* have established certain limits for the numbers $m_i{}^j$ for λ prime, and for a field of order q. Corresponding limits may be shown to hold for any field by their methods, provided λ is prime. The value of $m_0{}^0$ given above coincides with the upper or lower limit which they have obtained according as s is odd or even.

We shall show that equations (10) are also true if λ is composite. In view of Theorem 1, we may do this by showing that the values given by (10) satisfy equations (5), § 3. A sum $M_{a,b,0}$ having the value given by (5a) contains $m_0{}^0$, $a' - 1$ numbers $m_0{}^i$, $b' - 1$ numbers $m_i{}^0$, $d' - 1$ numbers $m_i{}^i$, and $\lambda - a' - b' - d' + 2$ numbers $m_i{}^j$, where $i \not\equiv 0$, $j \not\equiv 0$, $i \not\equiv j$, mod λ. When the values given by (10) are substituted, the result is found to coincide with the known value given by (5a). We find the same to be true in the other four cases, distinguished according to the divisibility of c by a', b', d'.

We therefore have

Theorem 2. *If $q^{t_1} \equiv -1$, mod λ, and $t = st_1$, the values of the numbers $m_i{}^j$ for a field of order q^{2t} are given by equations* (10).

A relation between the numbers $m_i{}^j$ for different fields.

5. We suppose now that $q^t \equiv 1$, mod λ, and denote by ${}_sm_i{}^j$ and $m_i{}^j$ the numbers of solutions of the congruences for the fields of order q^{st} and q^t respectively. We suppose also that the primitive roots g_s and g in these two fields are so chosen that $g_s{}^{\nu_s} \equiv g^\nu$, where

$$\nu_s = \frac{q^{st} - 1}{\lambda}, \qquad \nu = \frac{q^t - 1}{\lambda}.$$

In the author's previous paper† it was shown that, if this condition is satisfied, the cyclotomic functions for the two fields are connected by the relation

$$(1) \qquad \sum_{i,j} {}_sm_i{}^j\alpha^{aj+bi} = (-1)^{s-1}\{\sum_{i,j} m_i{}^j\alpha^{aj+bi}\}^s,$$

* L. c.

† L. c., p. 176.

where, as above, α denotes a primitive λth root of unity, a, b are any two integers such that $a \not\equiv 0$, $b \not\equiv 0$, $a + b \not\equiv 0$, mod λ, and i, j range independently over the residues $0, 1, 2, \cdots, \lambda - 1$.

The relation (1) also holds if one of the congruences $a \equiv 0$, $b \equiv 0$, $a + b \equiv 0$, mod λ, is satisfied. For in that case the value of each of the functions is -1 unless q and ν (or ν_s) are both odd, $a \equiv 0$, mod λ, and b is odd, in which case it is $+1$.* But if q and ν are both odd, then ν_s is odd or even with s, and hence the value of the function for the field of order q^{st} is $(-1)^{s-1}$.

If we replace α by α^k and suppose that $dv(\lambda, a, b) = 1$, we may write equation (1) in the form

$$\sum_c {}_sM_{a,b,c}\alpha^{kc} = (-1)^{s-1}\sum_c S_{a,b,c}\alpha^{kc}, \tag{2}$$

where k has any residue, mod λ, except 0, ${}_sM_{a,b,c}$ denotes the sum of the numbers ${}_sm_i^j$ for which

$$aj + bi \equiv c, \qquad \text{mod } \lambda,$$

and $S_{a,b,c}$ denotes the sum of all products of the form

$$m_{i_1}^{j_1} m_{i_2}^{j_2} \cdots m_{i_s}^{j_s}, \tag{3}$$

where the indices assume all residues as values, mod λ, for which

$$a(j_1 + j_2 + \cdots + j_s) + b(i_1 + i_2 + \cdots + i_s) \equiv c, \qquad \text{mod } \lambda.$$

For $k \equiv 0$, mod λ, we may write, in view of equations (2), § 3,

$$\sum_c {}_sM_{a,b,c} = q^{st} - 2 + (-1)^s(q^t - 2)^s + (-1)^{s-1}\sum_c S_{a,b,c}. \tag{2'}$$

From the equations (2), (2') we obtain

$${}_sM_{a,b,c} = \frac{1}{\lambda}[q^{st} - 2 + (-1)^s(q^t - 2)^s] + (-1)^{s-1}S_{a,b,c}.$$

We observe that equations (5), § 3, will all be satisfied provided the numbers ${}_sm_i^j$ have the values

$${}_sm_i^j = \frac{1}{\lambda^2}[q^{st} - 2 + (-1)^s(q^t - 2)^s] + (-1)^{s-1}s_i^j, \tag{4}$$

where s_i^j denotes the sum of all the products of the form (3) for which

$$i_1 + i_2 + \cdots + i_s \equiv i, \qquad j_1 + j_2 + \cdots + j_s \equiv j, \qquad \text{mod } \lambda.$$

In view of Theorem 1, we have therefore

Theorem 3. *If $q^t \equiv 1$, mod λ, and if the primitive roots g_s and g in the fields of order q^{st} and q^t be so chosen that $g_s^{\nu_s} \equiv g^\nu$, then the numbers ${}_sm_i^j$ for the field of order q^{st} may be expressed in terms of the numbers m_i^j for the field of order q^t by means of equations* (4).

UNIVERSITY OF PENNSYLVANIA,
PHILADELPHIA, PA.

* This may be shown by means of equations (1) and (2), § 3, of the present paper.

ON THE GEODESICS AND GEODESIC CIRCLES ON A DEVELOPABLE SURFACE.*

By William Caspar Graustein.

1. If a geodesic† on a developable surface is given parametrically, in terms of its arc s, by $x = x(s)$,‡ the developable is its rectifying developable and is given, in terms of s and a second parameter, η, by

$$y = x + \eta\left(\frac{R}{T}\alpha - \gamma\right). \tag{1}$$

The treatment in this paper depends upon this means of representing a developable surface.§ If the developable is so given, equations mapping it isometrically upon a plane are easily found. Thus the geodesics and geodesic circles on the developable are determined and formulæ and theorems for them obtained. Algebraic geodesics and geodesic circles are discussed, the intrinsic equations of the geodesic circles on cylinders and cones are set up and the cylinders on which there exist geodesic circles of constant curvature are determined.

The treatment holds for every type of developable, in that (1) is based, not on the developable, but on a geodesic on it. Furthermore, since this geodesic is an arbitrary one on the developable, a general theorem, proved for it, holds for every other one.

2. The ratio of the curvature to the torsion of a geodesic of (1) equals the tangent of the angle under which it intersects the ruling; for if Φ $(0 \leq \Phi < \pi)$ is this angle for the "x-curve," then

$$\tan \Phi = \frac{T}{R}.$$

The direction of the ruling, in terms of Φ, is $\alpha \cos \Phi - \gamma \sin \Phi$, and that of the normal to the surface, suitably oriented, is β.

If η is a function of s, (1) represents the general curve (not a ruling) on

* Read before the American Mathematical Society, January 2, 1915.

† The rulings of the developable are not considered as geodesics.

‡ In this paper x_1, x_2, x_3 are the coördinates of the point x; $x_1 = x_1(t)$, $x_2 = x_2(t)$, $x_3 = x_3(t)$ is the parametric representation of the curve $x = x(t)$; $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3, \gamma_1, \gamma_2, \gamma_3$ are the direction cosines of the directions α, β, γ of the tangent, principal normal and binormal; R and T are the radii of curvature and torsion.

§ This representation was used by Enneper, "Zur Theorie der Curven doppelter Krümmung," Mathematische Annalen, Bd. 19 (1882), pp. 72–78, to determine the natural equation of the geodesics on a developable which has as edge of regression a given type of curve.

the surface. The formulæ for this curve, on the introduction of the symbols, ξ, A, B, as follows:

$$s + \eta \cot \Phi = \xi, \qquad \xi'\eta'' - \xi''\eta' = A,$$

$$1 + \eta \frac{d}{ds}(\cot \Phi) = \xi' - \eta' \cot \Phi = B,$$

where the primes denote differentiation with respect to s, are

$$ds_y = \sqrt{\xi'^2 + \eta'^2}\, ds,$$

$$\sqrt{y' \mid y'}\, \alpha_y = \xi'\alpha - \eta'\gamma,$$

$$\sqrt{y' \mid y'}\, \sqrt{y'y'' \mid y'y''}\, \beta_y = -A\eta'\alpha + \frac{B}{R}(\xi'^2 + \eta'^2)\beta - A\xi'\gamma, \tag{2}$$

$$\sqrt{y'y'' \mid y'y''}\, \gamma_y = \frac{B}{R}\eta'\alpha + A\beta + \frac{B}{R}\xi'\gamma,$$

where

$$(y' \mid y') = \xi'^2 + \eta'^2, \qquad (y'y'' \mid y'y'') = A^2 + \frac{B^2}{R^2}(\xi'^2 + \eta'^2).*$$

Finally, the geodesic curvature of the curve is

$$\frac{1}{r_y} = \frac{(\gamma_y \mid \beta)}{R_y} = \frac{A}{(\xi'^2 + \eta'^2)^{\frac{3}{2}}}. \tag{3}$$

The edge of regression of the developable (if it has one) is given by $B = 0$. For the real points of one sheet of a real developable $B > 0$, and for those of the other sheet, $B < 0$. The x-curve lies wholly on one sheet (if $\eta = 0$, then $B = 1$); hence so does every geodesic.

3. By (2), the curves $\eta = \text{const}$ and the x-curve, $\eta = 0$, have parallel tangents and principal normals in corresponding points, that is, in points on the same ruling. Hence the curves $\eta = \text{const}$ are geodesics on the developable, such that when the developable is applied to the plane they become parallel lines. Accordingly, they shall be called a family of parallel geodesics. Their orthogonal trajectories form a second family of parallel geodesics, given, as is evident from (2), by $\xi = s + \eta \cot \Phi = \text{const}$. Now if the orthogonal system of geodesics, $\xi = \text{const}$, $\eta = \text{const}$, is made parametric, with ξ, η as the parameters, the linear element of the surface becomes $ds^2 = d\xi^2 + d\eta^2$. Hence the equations

$$\xi = s + \eta \cot \Phi, \qquad \eta = \eta \tag{4}$$

define an isometric map of the developable (1) on the (ξ, η) plane.

* And

$$(y' \mid y') = y_1'^2 + y_2'^2 + y_3'^2,$$

$$(y'y'' \mid y'y'') = (y_2'y_3'' - y_3'y_2'')^2 + (y_3'y_1'' - y_1'y_3'')^2 + (y_1'y_2'' - y_2'y_1'')^2.$$

4. If a geodesic on a developable is considered as a line of shortest distance and a geodesic circle as the locus of a point moving (on the surface) at a fixed geodesic distance from a given point of the surface, their finite equations are, according to the map (4),

$$c_1 + c_2\eta + c_3\xi = 0, \tag{5}$$

$$(\xi - \xi_0)^2 + (\eta - \eta_0)^2 = r^2. \tag{6}$$

The geodesics may, however, be considered as the curves of zero geodesic curvature, or as the curves with principal normals normal to the surface. Either of these points of view leads simply to the differential equation, $A = \xi'\eta'' - \xi''\eta' = 0$, whose integral may be put in the form (5). It will be better to use, instead of (5),

$$\eta = \tan\varphi(\xi - k), \tag{7}$$

though in so doing the geodesics $\eta = \text{const}$ are ruled out. Evidently φ is the angle, suitably measured, between the geodesic and the x-curve, and k determines its point of intersection with the x-curve. Thus the curves $\varphi = \text{const}$ are parallel geodesics cutting the geodesics $\eta = \text{const}$ under the (constant) angle φ; the curves $k = \text{const}$ are the geodesics passing through the fixed point $s = k$ of the x-curve.

For a developable surface geodesic circles may be defined as above or as curves of non-vanishing constant geodesic curvature.* Thus, from (3), their differential equation is

$$r(\xi'\eta'' - \xi''\eta') = (\xi'^2 + \eta'^2)^{\frac{3}{2}}. \tag{8}$$

If for ξ' is set $\eta' \cot\varphi$, and then again, for η', $\xi' \tan\varphi$, where φ is now considered as a function of s, there results, first,

$$\xi' = \varphi' r\cos\varphi, \qquad \eta' = \varphi' r\sin\varphi, \tag{9}$$

and hence the two equations, equivalent to (6):

$$\xi - \xi_0 = r\sin\varphi, \qquad \eta - \eta_0 = -r\cos\varphi. \tag{10}$$

5. The general geodesic w (not one of the family $\eta = \text{const}$) is

$$w = x + \frac{s - k}{\cot\varphi - \cot\Phi}(\alpha\cot\Phi - \gamma).$$

The formulæ (2) become, for this geodesic,

$$ds_w = \eta'\csc\varphi ds,$$

$$\alpha_w = \alpha\cos\varphi - \gamma\sin\varphi, \qquad \beta_w = \beta, \qquad \gamma_w = \alpha\sin\varphi + \gamma\cos\varphi. \tag{11}$$

* The two definitions lead to the same curves only for surfaces of constant total curvature.

By application of the Frenet-Serret formulæ R_w and T_w are found:

$$\frac{1}{R_w} = \frac{\sin^2(\Phi - \varphi)}{\sin^2 \Phi} \frac{1}{BR}, \qquad \frac{1}{T_w} = \frac{\sin 2(\Phi - \varphi)}{\sin 2\Phi} \frac{1}{BT}. \tag{12}$$

If Φ_w, where $\cot \Phi_w = R_u/T_w$, is introduced, evidently

$$\cot \Phi_w = \cot(\Phi - \varphi), \qquad \text{or} \qquad \Phi_w = \Phi - \varphi, \qquad -\pi < \Phi_w < \pi.$$

Then the formulæ (12) for the curvature and torsion become

$$R_w \sin^2 \Phi_w = BR \sin^2 \Phi, \qquad T_w \sin 2\Phi_w = BT \sin 2\Phi.$$

From the first formula Euler's equation for normal curvatures in a parabolic point may be reduced. A similar equation for the torsions of the geodesics in a point follows from the second formula.

By means of the formulæ (12) it is easy to establish the following results.*

The product of the curvatures of two orthogonal geodesics in a point equals the square of the torsion of either in the point.

As a geodesic rotates about a point, the rate of change of its curvature with respect to the angle of rotation is twice the torsion of the geodesic in the point:

$$\frac{\partial}{\partial \varphi}\left(\frac{1}{R_u}\right) = -\frac{2}{T_w}. \tag{13}$$

If the radius of curvature, R, of the x-curve (lying wholly on the sheet $B > 0$ of the surface) is taken as never negative, the curvature of an arbitrary curve of the surface in a point of the sheet $B > 0$ is never negative, and, in a point of the sheet $B < 0$, never positive.

6. The ratio of the curvature of a geodesic to its torsion has been shown equal to the tangent of the angle under which the geodesic cuts the ruling. Geometric interpretations may be obtained also for the derivative and the logarithmic derivative of this ratio, by introducing the edge of regression of the developable,

$$X = x - \frac{\alpha \cot \Phi - \gamma}{\frac{d}{ds}(\cot \Phi)}. \tag{14}$$

If a point p trace the geodesic with unit velocity, and P is the point on the edge of regression corresponding to p, that is, lying on the same ruling, the rate of change of the ratio in p equals the negative reciprocal of the distance of P from the osculating plane in p, and its logarithmic rate of change equals the reciprocal of the distance of P from the normal plane in p.

Now, from (14), the developable is, (a) a cylinder, if and only if the

* The first of these is true, for a general surface, in any parabolic point; the second, in any non-singular point.

ratio in question is constant,* and (*b*) a cone, if and only if the derivative of the ratio with respect to the arc of the geodesic is constant, not zero.† The geometric interpretation of the ratio and its derivative may be introduced here to obtain geometric criteria for cylinders and cones.‡

7. The general geodesic circle z on the developable (1) is

$$z = x + \eta(\alpha \cot \Phi - \gamma),$$

where s and η are connected by (6), or better, are given, by (10), in terms of φ. Now φ, for a point of the geodesic circle z, measures the angle under which it meets the curve $\eta = \text{const}$ through the point, just as it did for the geodesic w; for, by (9), the α_y of (2) becomes $\alpha_w = \alpha \cos \varphi - \gamma \sin \varphi$. But for the geodesics φ was an arbitrary constant, and here it is an auxiliary variable. And since φ entered into (7) only in cot φ, there it could be restricted to the interval $0 \leq \varphi < \pi$; on the other hand (10) contains sin φ, cos φ, so that here φ can at most be restricted to the interval $0 \leq \varphi < 2\pi$. Thus through a given point in a given (unoriented) direction on the developable there pass two geodesic circles of given geodesic curvature.

From (9) and (2), by means of (8) and (12),

$$(z'|z') = \xi'^2 + \eta'^2 = r^2\varphi'^2 = \frac{BR_w}{R}, \qquad rA = (z'|z')^{\frac{1}{2}}.$$

By means of these formulæ (2), in conjunction with (11), gives

$$\frac{1}{R_z^2} = \frac{1}{R_w^2} + \frac{1}{r^2}, \tag{15}$$

$$\alpha_z = \alpha_w, \qquad \frac{\beta_z}{R_z} = \frac{\beta_w}{R_w} - \frac{\gamma_w}{r}, \qquad \frac{\gamma_z}{R_z} = \frac{\beta_w}{r} + \frac{\gamma_w}{R_w}.$$

Thus the curvature and the directions of the trihedral of the geodesic circle z in a point are expressed in terms of the corresponding quantities for the geodesic w, tangent to it in the point.§ The first relation says that the difference of the squares of the curvature and geodesic curvature of a geodesic circle in a point depends only on its direction there. Further, the two geodesic circles in the same direction in a point with the same geodesic

* This was first shown by de Saint-Venant, "Sur les lignes courbes non planes," Journal de l'ecole polytechnique, vol. 30 (1845).

† This was first proved by Enneper, "Bemerkungen über Curven doppelter Krümmung," Göttingener Nachrichten, 1886, pp. 134–140.

‡ One of the two for the cone is given by Pirondini, "Sulle linee a doppia curvatura," Giornale di Matematiche di Battaglini, vol. 26 (1888), p. 105 ff.

§ These relations hold for an arbitrary curve on the general surface as the "z-curve" and the normal section tangent to it as the "w-curve" and may be obtained directly from Meusnier's theorem and the definition of geodesic curvature.

curvature have the same curvature; their principal normals are equally inclined, on opposite sides, to the normal of the surface.

8. The torsion of the geodesic circle z plus the derivative, with respect to its arc, of the angle ψ_z, which its osculating plane makes with the tangent plane to the surface, equals the torsion of the tangent geodesic w:

$$\frac{1}{T_z} + \frac{d\psi_z}{ds_z} = \frac{1}{T_w}, \qquad \text{where} \qquad \cos\psi_z = (\gamma_z|\beta_w) = \frac{R_z}{r}.* \tag{16}$$

Hence

$$\frac{1}{T_z} = \frac{1}{T_w} - \frac{R_z R_w}{r}\frac{d}{ds_z}\left(\frac{1}{R_z}\right).$$

Differentiation of (15) yields

$$\frac{R_z}{R_w}\frac{d}{ds_z}\left(\frac{1}{R_z}\right) = \frac{d}{ds_w}\left(\frac{1}{R_w}\right) + \frac{d\varphi}{ds_z}\frac{\partial}{\partial\varphi}\left(\frac{1}{R_w}\right) = \frac{d}{ds_w}\left(\frac{1}{R_w}\right) - \frac{2}{rT_w},$$

where (13) and the relation $rd\varphi = ds_z$ are used to obtain the final form. Thus the torsion of the geodesic circle is

$$\frac{1}{T_z} = \frac{1}{T_w}\left(1 + 2\frac{R_z^2}{r^2}\right) - \frac{R_z^2}{r^2}\frac{d}{ds_w}\left(\frac{r}{R_w}\right). \tag{17}$$

If φ is increased by π, the last term on the right changes sign, the first term does not. Thus the two geodesic circles in the same direction in a point with the same geodesic curvature have the same torsion only if their common tangent geodesic behaves in the point like a curve of constant curvature, and the same torsion except for sign only if it behaves there like a plane curve. Any two such geodesic circles on a circular cylinder have the same torsion in the point of contact. Finally, inspection shows that the torsions of two geodesic circles in two oriented directions making equal angles with the ruling are equal except for sign.

9. For a particular type of developable given, it is possible to build up from the intrinsic equation of its geodesics and the relation (16), or (17), the natural equation of its geodesic circles, by the use of (15), (12) and the formula $s_z = r\varphi$. Thus for the circular cylinder of radius a, the intrinsic equations of its individual geodesic, $T\sin 2\Phi = 2a$, $R\sin^2\Phi = a$, and the relation (17) yield the intrinsic equations of its geodesic circles,

$$\frac{1}{T_z} - \left(1 + 2\frac{R_z^2}{r^2}\right)\frac{\sin 2\left(\frac{s_z}{r} - \Phi\right)}{2a} = 0,$$

and the intrinsic equations of its individual geodesic circle,

$$\frac{1}{R_z^2} = \frac{1}{r^2} + \frac{\sin^4 t}{a^2}, \qquad \frac{1}{T_z} = \frac{r^2\sin^4 t + 3a^2}{r^2\sin^4 t + a^2}\frac{\sin 2t}{2a}, \qquad t = \Phi - \frac{s_z}{r}.$$

* This is Bonnet's formula for the geodesic torsion of a curve on an arbitrary surface. Cf. Eisenhart, Differential Geometry, p. 138.

The intrinsic equation of the geodesic circles on an arbitrary cylinder, for which the intrinsic equation of the geodesics is $\cot \Phi = \text{const}$, is obtained similarly as

$$\frac{1}{T_z} + \frac{d\psi_z}{ds_z} + \frac{\sin \psi_z}{R_z} \cot\left(\frac{s_z}{r} - \Phi\right) = 0.$$

Evidently, if the curvature of a geodesic circle is constant, its torsion is proportional to the cotangent of the ratio of its arc to its radius of geodesic curvature. Further, it may be shown, that there exists one (and hence ∞^1) such geodesic circles on the cylinder only if the intrinsic equation of the directrix may be put in the form, $\bar{R}\, r \tan \psi_z = r^2 - \bar{s}^2$,* where ψ_z is constant.

The intrinsic equation of the geodesic circles on a cone, whose geodesics are given by $ds - c\, d(\cot \Phi) = 0$, turns out to be

$$\frac{dK_z}{ds_z} + \frac{\sin K_z \sin\left(K_z + \dfrac{s_z}{r}\right)}{c + \eta_0 - r \cos \dfrac{s_z}{r}} + \frac{1}{r} = 0, \qquad \text{where} \qquad \cot K_z = \frac{\dfrac{1}{T_z} + \dfrac{d\psi_z}{ds_z}}{\dfrac{\sin \psi_z}{R_z}}.$$

In fact, this determines the geodesics or the geodesic circles according as r is finite or becomes infinite, and applies to the cone when c is finite, to the cylinder when c becomes infinite.

10. A curve is algebraic if it can be expressed parametrically by algebraic functions, and is algebraically rectifiable if it can be so expressed in terms of its arc.

It follows, from (1), that a developable is algebraic, if a single geodesic on it is algebraic; and from (7), that if two non-parallel geodesics are algebraic or if a single geodesic is algebraically rectifiable, every geodesic is not only algebraic but also algebraically rectifiable.*

Inspection of (6) shows further: (*a*) if a geodesic and a geodesic circle are algebraic, every geodesic and every geodesic circle is algebraic; (*b*) if the geodesics are algebraic, the geodesic circles are algebraic—but not algebraically rectifiable, since s_z is algebraic or not with φ ($s_z = r\varphi$), and the trigonometric functions of φ are algebraic.

* Here $\bar{R}$ is a non-definite quadratic polynomial in $\bar{s}$; the curves for which $\bar{R}$ is a definite quadratic polynomial in $\bar{s}$ are the alysoids (e. g., the catenary) of Cesàro, Nouvelles Annales de Mathématiques, 1886, p. 75.

* Cf. Stäckel, "Über algebraisch rectificierbare Raumkurven," Mathematische Annalen, Bd. 43 (1893), p. 171 ff., where this last result is found as an application of a theory of algebraically rectifiable space curves, developed largely by means of the properties of involutes and evolutes.

NOTE ON REPRESENTATIONS OF THE PARTIAL SUM OF A FOURIER'S SERIES.

By Dunham Jackson.

The problem of the convergence of expansions in series associated with ordinary linear differential equations has been developed with a high degree of generality by Birkhoff* and others. It is a characteristic of the method employed that the sum of the first n terms of the series is represented by a contour integral in the plane of the complex parameter. For the fundamental particular case of Fourier's series, it is a somewhat interesting exercise to derive the ordinary real formula for the partial sum directly from the contour integral, without going back to the individual terms which make up the sum. Of course no new conclusions are reached, and no novel methods are required; the most that is new is the opening of a fresh path through a much-traversed region. Two parallel discussions are given below, corresponding to the alternative systems, one of the first order and one of the second, from which the Fourier development is obtained.

I. System of the first order.

Let us begin with the system composed of the differential equation

$$\frac{du}{dx} + \lambda u = 0$$

and the boundary condition

$$u(0) = u(2\pi).$$

Its characteristic numbers are the numbers $\lambda = ki$, $k = 0, \pm 1, \pm 2, \cdots$, and the corresponding characteristic functions have the form

$$u_k(x) = e^{-kix}.$$

They lead to the expansion of an arbitrary function $f(x)$ in a series of the form

$$\sum_{k=-\infty}^{+\infty} a_k u_k(x),$$

where†

* Transactions of the American Mathematical Society, vol. 9 (1908), pp. 373–395.

† The value of the integral in the denominator is of course found to be simply 2π, when the explicit expressions for $u_k(t)$ and $v_k(t)$ are inserted.

$$a_k = \frac{\int_0^{2\pi} f(t)v_k(t)dt}{\int_0^{2\pi} u_k(t)v_k(t)dt},$$

the functions

$$v_k(x) = e^{kix}$$

being the characteristic solutions of the adjoint system

$$-\frac{dv}{dx} + \lambda v = 0, \qquad v(0) = v(2\pi).$$

In this form, the series does not appear strikingly familiar; but on combining the terms whose indices are the negatives of each other, and expressing the exponentials in terms of trigonometric functions, it is found that

$$a_k u_k(x) + a_{-k}u_{-k}(x) = \frac{1}{\pi}\cos kx \int_0^{2\pi} f(t)\cos ktdt + \frac{1}{\pi}\sin kx \int_0^{2\pi} f(t)\sin ktdt,$$

so that the given system does really lead to the ordinary Fourier's series.*

The Green's function of the system, $G(x, s, \lambda)$, is

$$(1) \qquad \frac{e^{\lambda(s-x)}}{1-e^{-2\lambda\pi}}, \quad x > s; \qquad \frac{e^{\lambda(s-x-2\pi)}}{1-e^{-2\lambda\pi}}, \quad x < s.$$

This may be found, for example, by direct substitution in the general determinant formula.† In accordance with the general theory, the sum of the first terms of the series is given by

$$\sum_{k=-n}^{+n} a_k u_k(x) = \frac{1}{2\pi i}\int_0^{2\pi} f(s)\int_C G(x, s, \lambda)d\lambda ds;$$

the integral is extended around a contour in the λ-plane presently to be specified. Our problem, then, may be stated in the following form, which is intelligible on its own merits, quite apart from the general considerations that have led up to it:

To establish the identity

$$(2) \qquad \frac{1}{2\pi i}\int_C G(x, s, \lambda)d\lambda = \frac{1}{\pi}\frac{\sin(n+\frac{1}{2})(s-x)}{2\sin\frac{1}{2}(s-x)},$$

where G is the function defined by (1), *and C is a contour inclosing the points* $0, \pm i, \pm 2i, \cdots, \pm ni$, *in the λ-plane, but no other roots of the denominator of G.*

* Cf. Birkhoff, loc. cit., p. 389.

† Cf. Birkhoff, loc. cit., p. 378.

Beyond the requirement just stated, the exact form of the contour is without effect on the value of the integral, since the integrand is analytic except where the denominator vanishes; but it does have an influence on the ease of actually performing the calculation. We shall find it convenient to use for C the rectangle having its vertices at the points $\pm g \pm (n + \frac{1}{2})i$, where n has the value which appears in (2), and g is an arbitrary positive real quantity, which will be allowed to increase without limit in the course of the proof. We shall let M, N, P, Q denote the corners of the rectangle in the first, second, third and fourth quadrants respectively.

For our purposes, no significance attaches to the variables s and x separately; we may introduce a single letter for the quantity

$$s - x = t.$$

Then we have to consider separately the cases that $-2\pi < t < 0$, $0 < t < 2\pi$. It appears that no provision is made hereby for the values $t = 0, \pm 2\pi$; but with regard to these, it suffices to remark that the integral which forms the left-hand member of (2) is obviously a continuous function of t.

Suppose first that $t < 0$.

On the upper side MN of the rectangle, we may set*

$$\lambda = u + (n + \tfrac{1}{2})i;$$

the imaginary part is constant, and the real part u varies from $+g$ to $-g$. On making the substitution in the integral, it appears that

$$\int_M^N \frac{e^{\lambda t}}{1 - e^{-2\lambda\pi}}\, d\lambda = e^{(n+\frac{1}{2})it} \int_{+g}^{-g} \frac{e^{ut}}{1 + e^{-2u\pi}}\, du.$$

In the same way,

$$\int_P^Q \frac{e^{\lambda t}}{1 - e^{-2\lambda\pi}}\, d\lambda = e^{-(n+\frac{1}{2})it} \int_{-g}^{+g} \frac{e^{ut}}{1 + e^{-2u\pi}}\, du.$$

So the integral about the whole contour has the expression

$$(3) \quad \int_C G d\lambda = [e^{-(n+\frac{1}{2})it} - e^{(n+\frac{1}{2})it}] \int_{-g}^{+g} \frac{e^{ut}}{1 + e^{-2u\pi}}\, du + \int_Q^M G d\lambda + \int_N^P G d\lambda.$$

The right-hand member may be replaced by its limit for $g = \infty$, since its value is independent of g. We shall see that the second and third integrals separately approach zero; it will follow that the first term approaches a limit as g becomes infinite (a fact which is readily established

* The use of the letter u here is independent of that in the first few lines of the section.

directly), and that the value of this limit is the value of the contour integral.

Consider the side QM. If we set

$$\lambda = g + vi, \quad -(n + \tfrac{1}{2}) \leqq v \leqq n + \tfrac{1}{2},$$

then

$$| e^{-2\lambda\pi} | = e^{-2g\pi},$$

and

$$| 1 - e^{-2\lambda\pi} | \geqq 1 - e^{-2g\pi} > \tfrac{1}{2},$$

if g is sufficiently large. On the other hand,

$$| e^{\lambda t} | = e^{gt} = e^{-g|t|},$$

and this approaches zero as g becomes infinite, so that the first member approaches zero uniformly throughout the finite range of variation of v, for any particular value of t. The same thing therefore is true of G, and the statement with regard to the second integral on the right of (3) is justified. By writing

$$G = \frac{e^{\lambda t}}{1 - e^{-2\lambda\pi}} = \frac{e^{\lambda(t+2\pi)}}{e^{2\lambda\pi} - 1},$$

and setting

$$\lambda = -g + vi$$

along the side NP, we may apply similar reasoning to the third term. We recognize thus that

$$\int_C G d\lambda = -2i \sin\{(n + \tfrac{1}{2})t\} \int_{-\infty}^{+\infty} \frac{e^{ut}}{1 + e^{-2u\pi}}\, du, \tag{4}$$

in which the bracket factor from (3) has been replaced by an equivalent simpler expression. It is noticeable that the index n no longer appears under the sign of integration.

Let

$$J = \int_{-\infty}^{+\infty} \frac{e^{ut}}{1 + e^{-2u\pi}}\, du, \qquad J_g = \int_{-g}^{+g} \frac{e^{ut}}{1 + e^{-2u\pi}}\, du.$$

Introducing a new complex variable z, let us consider the integral of the function

$$\frac{e^{zt}}{1 + e^{-2z\pi}}$$

extended in the positive direction around the rectangle in the z-plane whose vertices R, S, T, U are the points $g + i$, $-g + i$, $-g$, $+g$ respectively. The integrand is analytic throughout the rectangle, except at the one point $z = \frac{1}{2}i$. There it has the residue $e^{\frac{1}{2}it}/2\pi$, as is seen by expanding the denominator in powers of $z - \frac{1}{2}i$, and performing the indicated division. The value of the contour integral accordingly is $ie^{\frac{1}{2}it}$.

Taking the sides of the rectangle one by one, we see first that the integral over TU is precisely J_g. On RS, we may set $z = \xi + i$, where ξ is real, and find that

$$\int_R^S \frac{e^{zt}}{1 + e^{-2z\pi}}\, dz = \int_{+g}^{-g} \frac{e^{\xi t} e^{it}}{1 + e^{-2\xi\pi}}\, d\xi = -e^{it} J_g.$$

Then

$$ie^{\frac{1}{2}it} = (1 - e^{it})J_g + J_g' + J_g'',$$

if the last two terms are understood to represent the integrals over the vertical sides of the rectangle. As at an earlier stage in the demonstration, we proceed to let g become infinite; it appears that J_g' and J_g'' approach zero, and*

$$ie^{\frac{1}{2}it} = (1 - e^{it})J, \qquad J = \frac{i}{e^{-\frac{1}{2}it} - e^{\frac{1}{2}it}} = -\frac{1}{2\sin\frac{1}{2}t}. \tag{5}$$

Combination of (4) and (5) gives for the original contour integral the expression

$$\int_C G d\lambda = \frac{i \sin\{(n + \frac{1}{2})t\}}{\sin\frac{1}{2}t}; \tag{6}$$

and on division by $2\pi i$ and substitution of the value of t, the desired identity is established, for the case that $-2\pi < t < 0$.

The other case, that $0 < t < 2\pi$, can be reduced immediately to the preceding. For if we set

$$t' = t - 2\pi = s - x - 2\pi,$$

the variable t' enters into the expression for the Green's function just as t entered before, and its range of variation is the same as that which was assigned to t before. The previous work is valid throughout, with t replaced by t'; and in the final formula (6), since the right-hand member, regarded as a function of t, has the period 2π, the accent may be dropped.

II. System of the second order.

Let us turn to the differential equation

$$\frac{d^2u}{dx^2} + \lambda u = 0,$$

with the pair of boundary conditions

$$u(0) = u(2\pi), \qquad u'(0) = u'(2\pi).$$

* Cf. Goursat, Cours d'analyse mathématique, vol. 2, exercise 15 at the end of Chapter XIV.

Instead of λ, we shall use for the most part the parameter ρ, defined by the equation

$$\rho^2 = \lambda.$$

The characteristic solutions are*

$$\cos kx, \qquad \sin kx, \qquad k = 0, 1, 2, \cdots.$$

The given system is self-adjoint, and the expansions associated with it are obtained immediately in the familiar form of Fourier's series. The expressions for the Green's function, when $x > s$ and when $x < s$, are respectively

$$\frac{\cos \rho(\pi + s - x)}{2\rho \sin \rho\pi}, \qquad \frac{\cos \rho(\pi + x - s)}{2\rho \sin \rho\pi}.$$

We shall be concerned with the integral

$$\int_C G d\lambda = \int_{C_1} 2\rho G d\rho,$$

the path of integration being a circuit in the λ-plane, or a half-circuit in the ρ-plane; the exact form which it will be convenient to use will be specified later.

As before, the cases $x > s$ and $x < s$ require discussions that are separate at the start, but speedily coalesce into one. If $x > s$, let $t = \pi + s - x$; if $x < s$, let $t = \pi + x - s$; then t is subject to the inequalities

$$-\pi < t < \pi$$

in either case, and in each case we have to evaluate the integral

$$\int_{C_1} \frac{\cos \rho t}{\sin \rho\pi} d\rho.$$

With regard to the path of integration, let M, N, P, Q be used, independently of the preceding section, to denote respectively the points $-gi$, $n + \frac{1}{2} - gi$, $n + \frac{1}{2} + gi$, gi. Then the integral is to be extended along the sides MN, NP, PQ, but *not* along the fourth side of the rectangle, since, as has been noticed already, a half-circuit in the ρ-plane corresponds to a complete circuit in the λ-plane. The value of the integral is independent of the value of g.

On the vertical side, let

$$\rho = n + \tfrac{1}{2} + vi,$$

* Of course the value $k = 0$ is to be excluded in the case of the sine.

where v is a real variable which goes from $-g$ to g. The denominator of the integrand assumes the form

$$\sin\{(n+\tfrac{1}{2}+vi)\pi\} = (-1)^n \cos v\pi i.$$

The numerator is

$$\cos\{(n+\tfrac{1}{2}+vi)t\} = \cos\{(n+\tfrac{1}{2})t\}\cos vti - \sin\{(n+\tfrac{1}{2})t\}\sin vti.$$

The factors $\cos\{(n+\frac{1}{2})t\}$, $\sin\{(n+\frac{1}{2})t\}$ are constant as far as the integration is concerned, and may be taken out before the integral sign. In the second term, the remaining factor $\sin vti$ is an odd function of v; and since the denominator $\cos v\pi i$ is even, the whole integrand is odd, and the corresponding term of the integral will vanish. For the significant part of the contour integral, we have the expression

$$\int_N^P \frac{\cos \rho t}{\sin \rho\pi} d\rho = i(-1)^n \cos\{(n+\tfrac{1}{2})t\} \int_{-g}^{+g} \frac{\cos vti}{\cos v\pi i} dv.$$

By setting $\rho = u \pm gi$, for the integration along the horizontal sides MN and PQ, and writing the trigonometric functions in terms of exponentials, it is readily seen that these integrals approach zero as g becomes infinite. It follows that

$$\int_{C_1} \frac{\cos \rho t}{\sin \rho\pi} d\rho = i(-1)^n \cos\{(n+\tfrac{1}{2})t\} \int_{-\infty}^{+\infty} \frac{\cos vti}{\cos v\pi i} dv.$$

The integral which remains in the right-hand member of the last relation can be reduced at once to that which was evaluated at the corresponding stage in the preceding section. In the first place,

$$\cos vti = \tfrac{1}{2}(e^{vt} + e^{-vt}),$$

and

$$\int_{-\infty}^{+\infty} \frac{e^{vt}}{\cos v\pi i} dv = \int_{-\infty}^{+\infty} \frac{e^{-vt}}{\cos v\pi i} dv,$$

as is seen by changing v into $-v$, so that

$$\int_{-\infty}^{+\infty} \frac{\cos vti}{\cos v\pi i} dv = \int_{-\infty}^{+\infty} \frac{e^{vt}}{\cos v\pi i} dv.$$

Then, if $\tau = t - \pi$, the new variable τ has the same range of values as t in the preceding section, and by making use of the earlier work we find that

$$\int_{-\infty}^{+\infty} \frac{e^{vt}}{\cos v\pi i} dv = 2\int_{-\infty}^{+\infty} \frac{e^{v(\tau+\pi)}}{e^{v\pi} + e^{-v\pi}} dv = 2\int_{-\infty}^{+\infty} \frac{e^{vt}}{1 + e^{-2v\pi}} dv = -\frac{1}{\sin \frac{1}{2}\tau}.$$

It remains only to combine and interpret the results that have been obtained. If $t = \pi + s - x$, then

$$\cos(n + \tfrac{1}{2})t = (-1)^{n+1} \sin(n + \tfrac{1}{2})(s - x),$$

$$\sin \tfrac{1}{2}\tau = \sin \tfrac{1}{2}(t - \pi) = \sin \tfrac{1}{2}(s - x),$$

$$\int_C G d\lambda = \int_{C_1} \frac{\cos \rho t}{\sin \rho\pi} d\rho = \frac{i \sin(n + \tfrac{1}{2})(s - x)}{\sin \tfrac{1}{2}(s - x)}.$$

If $t = \pi + x - s$, the only difference is that $s - x$ in the last formula is replaced by $x - s$, and this change has no effect on the value of the fraction.

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.

ACKNOWLEDGMENT.

BY FRANK IRWIN.

Professor Bôcher has called my attention to the fact that the contents of my note, "Relation between the roots of a rational integral function and its derivative," in the March, 1915, number of the *Annals* are substantially identical with the proof given by him in the *Annals*, vol. 7, 1892, page 70.

CERTAIN GENERAL PROPERTIES OF FUNCTIONS.*

By Henry Blumberg.

Introduction. Definitions and statement of results. Let $g(x)$ be a real, one-valued, bounded, continuous or discontinuous function defined in the interval (a, b). The functional values of $g(x)$ *in the subinterval* (α, β) of (a, b) have a least upper-bound, a greatest lower-bound and a saltus, which we denote respectively by

$$u(g, \alpha\beta),\ l(g, \alpha\beta) \text{ and } s(g, \alpha\beta) = u(g, \alpha\beta) - l(g, \alpha\beta).$$

The *upper-bound*, the *lower-bound*† and the *saltus* of $g(x)$ *at the fixed point* x of (a, b) are defined respectively as the (greatest) lower-bound of $u(g, \alpha\beta)$, the (least) upper-bound of $l(g, \alpha\beta)$ and the (greatest) lower-bound of $s(g, \alpha\beta)$ for all possible subintervals (α, β) of (a, b) that contain x as interior point.‡ With the given function $g(x)$, there are thus associated three new functions of x, *the upper-bound function, the lower-bound function* and *the saltus function*, which we denote by

$$u(g, x),\ l(g, x) \text{ and } s(g, x)$$

respectively.§ It is seen that

$$s(g, x) \equiv u(g, x) - l(g, x).$$

Let us, for the sake of brevity, write

$$s(g, x) \equiv s'(x), \qquad s(s', x) \equiv s''(x), \qquad s(s'', x) \equiv s'''(x), \ \cdots.$$

Sierpiński‖ has shown that

$$s''(x) \equiv s'''(x).$$

* Presented to the American Mathematical Society, April, 1914, and December, 1916.

† Throughout the paper, we use the expressions, "the upper-bound" and "the lower-bound," in the sense of "the least upper-bound" and "the greatest lower-bound," respectively.

‡ Of course, it will be understood, that in case $x = a$ or b—and only then—we permit α or β to coincide with x. This remark applies also to similar situations below.

§ The functions $u(g, x)$ and $l(g, x)$ are often, though not quite unobjectionably, called the "maximum" and the "minimum" functions belonging to $g(x)$. Cf., for example, Hobson, The Theory of Functions of a Real Variable (1907), art. 180.

‖ Bulletin de l'Acadèmie des Sciences de Cracovie (1910), pp. 633–634.

The chief aim of the present paper is to communicate a number of companion propositions to Sierpiński's theorem. The new results are based on the definition of other types of saltus, which immediately suggest themselves and arise from the one described above, when certain specified subsets of the range of the independent variable may be neglected.

The first new type arises when *finite* subsets may be neglected. For every subinterval (α, β) of (a, b), there evidently exists a number, which we denote by $u_f(g, \alpha\beta)$, uniquely characterized by the following double property:* For every $\epsilon > 0$, on the one hand, the set of points of the interval (α, β) for which $g(x) > u_f(g, \alpha\beta) + \epsilon$ is finite, while on the other hand, there exists an infinite set of points of (α, β) at which $g(x) > u_f(g, \alpha\beta) - \epsilon$. This number $u_f(g, \alpha\beta)$ is the lower-bound of all possible upper-bounds that $g(x)$ may have in the interval (α, β), in case a finite set of points may be neglected. Likewise, there is a number, which we denote by $l_f(g, \alpha\beta)$, characterized by the property that for every $\epsilon > 0$, the set of points of (α, β) where $g(x) < l_f(g, \alpha\beta) - \epsilon$ is finite, whereas, the set of points of (α, β) where $g(x) < l_f(g, \alpha\beta) + \epsilon$ is infinite. $l_f(g, \alpha\beta)$ is the upper-bound of all possible lower-bounds of $g(x)$ in (α, β), when a finite number of points may be neglected. Finally, we denote by $s_f(g, \alpha\beta)$ the lower-bound of the saltus of $g(x)$ in (α, β), in case a finite number of points may be neglected. Evidently

$$s_f(g, \alpha\beta) = u_f(g, \alpha\beta) - l_f(g, \alpha\beta).$$

We shall designate the numbers

$$u_f(g, \alpha\beta),\ l_f(g, \alpha\beta) \text{ and } s_f(g, \alpha\beta)$$

as "the *f-upper-bound*," "the *f-lower-bound*" and "the *f-saltus*" of $g(x)$ *in the interval* (α, β). As in the case where no point may be neglected, we now define "*the f-upper-bound*," "*the f-lower-bound*" and "*the f-saltus*" of $g(x)$ *at the fixed point* x of (a, b), as the lower-bound of $u_f(g, \alpha\beta)$, the upper-bound of $l_f(g, \alpha\beta)$ and the lower-bound of $s_f(g, \alpha\beta)$ for all possible subintervals (α, β) of (a, b) that contain x as interior point. With the given function $g(x)$, we have thus associated "*the f-upper-bound function*," "*the f-lower-bound function*" and "*the f-saltus function*," which we denote by

$$u_f(g, x),\ l_f(g, x) \text{ and } s_f(g, x)$$

respectively.

In the second place, the subsets that may be neglected are *denumerable*. As before, there exists a number, which we denote by $u_d(g, \alpha\beta)$, uniquely characterized by the property that, for every $\epsilon > 0$, the set of points of

* Cf. Baire, Acta Mathematica, vol. 30 (1906), pp. 21 and 22.

(α, β) where $g(x) > u_d(g, \alpha\beta) + \epsilon$ is denumerable, whereas the set of points where $g(x) > u_d(g, \alpha\beta) - \epsilon$ is non-denumerable; this number $u_d(g, \alpha\beta)$ we call *"the d-upper-bound"* of $g(x)$ in (α, β).* Precisely as before, we define the related numbers

$$l_d(g, \alpha\beta),\ s_d(g, \alpha\beta),\ u_d(g, x),\ l_d(g, x)$$

and *"the d-saltus function"* $s_d(g, x)$.

In the third place, *"exhaustible"* sets (i. e., sets of first category†) may be neglected. We then obtain "the *e-saltus function*" $s_e(g, x)$, together with the related numbers.

Finally, sets of (Lebesgue) *zero measure* may be neglected. We then obtain *"the z-saltus function"* $s_z(g, x)$, together with the related functions.

As in the case where no point may be neglected, we write

$$s_f(g, x) \equiv s_f'(x),\ s_f(s_f', x) \equiv s_f''(x),\ s_f(s_f'', x) \equiv s_f'''(x),\ \cdots;$$

and similarly for the d-saltus, the e-saltus and the z-saltus functions. Also

$$s_f'(x) = u_f(g, x) - l_f(g, x),$$

and similarly for the other saltus functions.

Having defined the new types of saltus we had in view, we may now state the corresponding analogues of Sierpiński's theorem. The most interesting and least obvious results are that

$$s_d'''(x) \equiv s_d^{\text{IV}}(x)$$

and

$$s_z'''(x) \equiv s_z^{\text{IV}}(x);$$

moreover, as examples show, $s_d''(x)$ and $s_z''(x)$ may be different from $s_d'''(x)$ and $s_z'''(x)$ respectively. In the case of the f-saltus, the functions $s_f^{(n)}(x)$ $(n = 1, 2, \cdots)$ may all be different. In the case of the e-saltus, it follows easily enough that $s_e'''(x)$ is always identically zero, whereas $s_e''(x)$ may be different from $s_e'''(x)$.

Because of our negative result in the case of the f-saltus, we are naturally led to define $s_f^{(\beta)}(x)$ for transfinite β's. Our result will show that it is sufficient to confine ourselves to transfinite ordinal numbers belonging to Cantor's second class. If β is not a limiting number, $\beta - 1$ exists, and we define $s_f^{(\beta)}(x)$ as equal to $s_f(s_f^{(\beta-1)}, x)$. For our purpose, therefore, all we have to do now is to define $s_f^{(\beta)}(x)$, in case β is a limiting number, in terms of the functions $s_f^{(\nu)}(x)$, where $\nu < \beta$. This we do simply by means of the equation

* It follows that the set of points of (α, β) for which $g(x) > u_d(g, \alpha\beta)$ is also denumerable. This fact may be used to modify our definition of the d-upper-bound. An analogous remark applies to the types of saltus defined below, but not, however, to the f-saltus.

† Cf. Denjoy, Journal de Mathématiques, ser. 7, vol. 1 (1915), pp. 122–125.

$$s_f^{(\beta)}(x) = \lim_{\nu_n \to \beta} s_f^{(\nu_n)}(x),$$

where $\{\nu_n\}$ is a sequence of numbers less than β. It is easily seen, especially in connection with our later discussion, that this limit always exists and is independent of the particularly chosen sequence $\{\nu_n\}$.

Our positive result for the case of the f-saltus may now be stated as follows:

There exists a number β of the first or the second class, such that

$$s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x).$$

Furthermore, it is shown by means of an example, that if β is a given number of the first or the second class, then the functions $s_f^{(\nu)}(x)$ $(1 \leqq \nu \leqq \beta)$ may all be different, whereas $s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x)$.

Attention is also directed to the relation

$$s_d(s_f'', x) \equiv s_f^{(\beta)}(x)$$

of § 4 connecting the f-saltus and the d-saltus.

For the sake of completeness, we include in our discussion the proof of Sierpiński's Theorem (§ 2). § 1 gives a lemma due to Baire, which simplifies later proofs. §§ 3, 4, 5, and 6 treat the d-saltus, the f-saltus, the e-saltus and the z-saltus respectively. The Appendix indicates generalizations.

1. A lemma due to Baire.* *Suppose that with each subinterval (α, β) of (a, b) there is associated a real number $\varphi_{\alpha\beta}$ in such a way that if (γ, δ) is contained in (α, β) we have $\varphi_{\gamma\delta} \leqq \varphi_{\alpha\beta}$; moreover, $\varphi_{\alpha\beta}$ has a finite lower-bound. Let $\varphi(x)$ be defined as the lower-bound of $\varphi_{\alpha\beta}$ for all possible intervals (α, β) containing x in their interior.† Then $\varphi(x)$ is an upper-semi-continuous function.*

That $\varphi(x)$ exists follows from the finiteness of the lower-bound of $\varphi_{\alpha\beta}$. Moreover, $\epsilon > 0$ having been given in advance, a subinterval (α, β) exists containing the fixed point x in its interior, such that $\varphi_{\alpha\beta} < \varphi(x) + \epsilon$. From our definition of $\varphi(x)$, we have for every point x_1 of (α, β):

$$\varphi(x_1) \leqq \varphi_{\alpha\beta} < \varphi(x) + \epsilon.$$

Hence $\varphi(x)$ is upper-semi-continuous at x.

By making $\varphi_{\alpha\beta}$ successively equal to $u(g, \alpha\beta)$, $u_f(g, \alpha\beta)$, $u_d(g, \alpha\beta)$, $u_e(g, \alpha\beta)$ and $u_z(g, \alpha\beta)$, we see that

$$u(g, x),\ u_f(g, x),\ u_d(g, x),\ u_e(g, x) \text{ and } u_z(g, x)$$

* Cf. Acta Mathematica, l. c., p. 16. Baire's situation is more general, but see Appendix.

† For the case where x is a or b, compare footnote above.

are upper-semi-continuous functions. Similarly, the functions $-l(g, x)$, $-l_f(g, x)$, etc., are upper-semi-continuous. Since the sum of two upper-semi-continuous functions is again upper-semi-continuous, it follows, in virtue of

$$s'(x) = u(g, x) - l(g, x), \quad s_f'(x) = u_f(g, x) - l_f(g, x),$$

etc., that

$$s'(x),\ s_f'(x),\ s_d'(x),\ s_c'(x), \text{ and } s_z'(x)$$

are upper-semi-continuous functions.

2. The ordinary saltus. THEOREM (Sierpiński).

$$s''(x) \equiv s'''(x) \equiv s^{\text{IV}}(x) \equiv \cdots.$$

Proof. According to § 1, $s'(x)$ is upper-semi-continuous and therefore continuous at every point of an everywhere dense subset $\mathfrak{S}$ of (a, b).* Since the saltus of a function is zero at its points of continuity, it follows that $s''(x)$, the saltus function belonging to $s'(x)$, is zero everywhere in $\mathfrak{S}$. Moreover, according to § 1, $s''(x)$, being a saltus function, is upper-semi-continuous and furthermore, everywhere $\geqq 0$. From the upper-semi-continuity of $s''(x)$, it follows that $u(s'', x)$, the upper-bound function belonging to $s''(x)$, is equal to $s''(x)$. From the fact that $s''(x) \geqq 0$ everywhere and $= 0$ at the points of $\mathfrak{S}$, it follows that $l(s'', x)$, the lower-bound function belonging to $s''(x)$, is identically zero. Therefore,

$$s'''(x) \equiv s(s'', x) \equiv u(s'', x) - l(s'', x) \equiv s''(x).$$

By taking $g(x)$ successively equal to $s'(x)$, $s''(x)$, $\cdots$, we see that

$$s'''(x) \equiv s^{\text{IV}}(x) \equiv s^{\text{V}}(x) \equiv \cdots.$$

3. The *d*-saltus. THEOREM. $s_d'''(x) \equiv s_d^{\text{IV}}(x) \equiv s_d^{\text{V}}(x) \equiv \cdots$.

The following example shows that $s_d''(x)$ need not equal $s_d'''(x)$. Let $(a, b) \equiv (0, 1)$; $g(x) = 0$, if x satisfies the inequalities $0 \leqq x \leqq \frac{1}{2}$, and is such that at most a finite number of 1's are present in its decimal development; $g(x) = 1$ at all other points of $(0, 1)$. It is seen that every subinterval of $(0, \frac{1}{2})$ has a non-denumerable number of points where $g(x) = 0$, and also a non-denumerable set of points where $g(x) = 1$. Hence,

$$s_d'(x) = 1 \ (0 \leqq x \leqq \tfrac{1}{2}), \quad s_d'(x) = 0 \ (\tfrac{1}{2} < x \leqq 1);$$

$$s_d''(x) = 0 \ (x \neq \tfrac{1}{2}), \qquad s_d''(\tfrac{1}{2}) = 1; \quad s_d'''(x) \equiv 0.$$

(This example may be modified so that $s_d''(x) \not\equiv s_d'''(x)$ and $s_d'''(x) \not\equiv 0$.)

We now proceed to the proof of the theorem. According to § 1,

* Cf., for example, Hobson, l. c., pp. 527 and 525.

$s_d'(x)$ is upper-semi-continuous and therefore continuous at every point of a set $\mathfrak{S}$, which contains in every subinterval of (a, b) a non-denumerable set of points.* At every point of continuity of $s_d'(x)$, we have $s(s_d', x) = 0$. Since it follows obviously from our definitions that

$$0 \leqq s_d(s_d', x) \leqq s(s_d', x),$$

we have $s_d(s_d', x) = s_d''(x) = 0$ at every point of $\mathfrak{S}$. This shows, in virtue of the non-negativity of $s_d''(x)$, that

$$l_d(s_d'', x) \equiv 0.$$

Moreover, since, according to § 1, $s_d''(x)$ is an upper-semi-continuous function,

$$u_d(s_d'', x) \leqq u(s_d'', x) \leqq s_d''(x).$$

Hence,

$$s_d'''(x) = u_d(s_d'', x) - l_d(s_d'', x) = u_d(s_d'', x) \leqq s_d''(x).$$

Now let $\mathfrak{R}''$ be the planar set of points whose coördinates are

$$x = x, \qquad y = s_d''(x) \quad (a \leqq x \leqq b).$$

If P is any point of the plane, *whether belonging to* $\mathfrak{R}''$ *or not*, then either there exists a neighborhood of P containing at most a denumerable subset of $\mathfrak{R}''$, or every neighborhood of P contains a non-denumerable subset of $\mathfrak{R}''$. In the first case, we call P a "*point of denumerability*" of $\mathfrak{R}''$; in the second case, a "*point of non-denumerability*" of $\mathfrak{R}''$.† We have just seen that $s_d'''(x) \leqq s_d''(x)$ everywhere. We show furthermore that *for every* ξ *of* (a, b), *the point* $(\xi, s_d'''(\xi))$ *is the highest point of non-denumerability of* $\mathfrak{R}''$ *on the line* $x = \xi$.‡ For suppose first that (ξ, η) is a point of denumerability of $\mathfrak{R}''$ such that every point in the line $x = \xi$ above (ξ, η) is also a point of denumerability of $\mathfrak{R}''$. We must then show that $s_d'''(\xi) < \eta$. Every point (ξ, y), $\eta \leqq y \leqq u(g, ab)$, being a point of denumerability of $\mathfrak{R}''$, may be enclosed in a rectangle with sides parallel to the coördinate axes containing in its interior and on its boundary at most a denumerable subset of $\mathfrak{R}''$. According to the Borel theorem on interval sets, no more than a finite number of distinct rectangles need to be used. It is then seen that, by taking δ sufficiently small, we may cut out from the region covered by these rectangles a region,

$$\xi - \delta \leqq x \leqq \xi + \delta, \qquad \eta - \delta \leqq y \leqq u(g, ab),$$

* See Hobson, l. c., pp. 527, 525, and 244.

† A "point of non-denumerability" is more usually called a "condensation point."

‡ The existence of such a point follows from the fact that the set of points of non-denumerability of $\mathfrak{R}''$ is closed. For our later purposes, it is sufficient to show merely that $(\xi, s_d'''(\xi))$ is a point of non-denumerability of $\mathfrak{R}''$.

containing in its interior and on its boundary at most a denumerable set of points. Therefore, the function $s_d''(x)$ has everywhere in the interval $(\xi - \delta, \xi + \delta)$ a value less than $\eta - \delta$ except possibly at the points of a denumerable set. Therefore, $u_d(s_d'', \xi) \leqq \eta - \delta$ and

$$s_d'''(\xi) = u_d(s_d'', \xi) \leqq \eta - \delta < \eta.$$

Secondly, suppose that (ξ, η) is a point of non-denumerability of $\mathfrak{R}''$. Then it is clear that $u_d(s_d'', \xi) \geqq \eta$ and

$$s_d'''(\xi) = u_d(s_d'', \xi) \geqq \eta.$$

This result, in conjunction with the inequality $s_d'''(\xi) < \eta$ in the previous case, shows that $(\xi, s_d'''(\xi))$ is actually the highest point of non-denumerability of $\mathfrak{R}''$ on the line $x = \xi$.

If, in particular, $(\xi, s_d''(\xi))$ is itself a point of non-denumerability of $\mathfrak{R}''$, it follows that $s_d'''(\xi) \geqq s_d''(\xi)$. In virtue of the inequality $s_d'''(\xi) \leqq s_d''(\xi)$ obtained above, it thus follows that

$$s_d'''(\xi) = s_d''(\xi)$$

for a point $(\xi, s_d''(\xi))$ of non-denumerability of $\mathfrak{R}''$.

According to a known theorem, the points of $\mathfrak{R}''$ that are points of denumerability of $\mathfrak{R}''$ constitute at most a denumerable set. Hence, if we designate by $\mathfrak{R}'''$ the set of points $(x, s_d'''(x))$, $a \leqq x \leqq b$, it follows from the fact that $s_d'''(\xi) = s_d''(\xi)$ when $(\xi, s_d''(\xi))$ is a point of non-denumerability of $\mathfrak{R}''$, that $\mathfrak{R}''$ and $\mathfrak{R}'''$ coincide except possibly at a denumerable set of points; and furthermore, that every point of non-denumerability of $\mathfrak{R}''$ is likewise a point of non-denumerability of $\mathfrak{R}'''$. But precisely as above, it is seen by use of $\mathfrak{R}'''$ instead of $\mathfrak{R}''$, that

$$s_d^{\text{IV}}(\xi) = s_d'''(\xi)$$

whenever $(\xi, s_d'''(\xi))$ is a point of non-denumerability of $\mathfrak{R}'''$. Since, however, according to the above, every point $(\xi, s_d'''(\xi))$ is a point of non-denumerability of $\mathfrak{R}''$, and therefore of $\mathfrak{R}'''$, it follows that for every x in the interval (a, b) the equation $s_d^{\text{IV}}(x) = s_d'''(x)$ holds.

As in the case of Sierpiński's theorem,

$$s_d^{\text{IV}}(x) \equiv s_d^{\text{V}}(x) \equiv \cdots.$$

Remark. *If* $s_{\aleph}'(x)$, $s_{\aleph}''(x)$, $s_{\aleph}'''(x)$, $\cdots$ *represent the successive saltus functions that arise when,* instead of neglecting denumerable sets (i. e., sets of cardinal number $\aleph_0$), *we neglect sets of cardinal number* $\aleph$, *where* $\aleph$ is any cardinal number $< c$, the cardinal number of the continuum, *then* $s_{\aleph}'''(x) \equiv s_{\aleph}^{\text{IV}}(x) \equiv \cdots$. The proof of this more general proposition, being entirely analogous to that of the special case $\aleph = \aleph_0$, is omitted.

4. The f-saltus. The following example shows that *if β is an ordinal number of the first or the second class, there exist functions $g(x)$, such that the functions $s_f^{(\nu)}(x)$ are all different for $1 \leqq \nu \leqq \beta$, whereas $s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x) \equiv \cdots$.* For let $\mathfrak{S}$ be a reducible set contained in the interval (a, b) such that $\mathfrak{S}^{(\beta)}$, the βth derivative of $\mathfrak{S}$, is the null-set, whereas every derivative $\mathfrak{S}^{(\nu)}$, $\nu < \beta$, contains points.* Let $g(x) = 1$ or 0 according as x belongs or does not belong to $\mathfrak{S}$. Clearly $s_f'(x) = 1$ or 0, according as x belongs or does not belong to $\mathfrak{S}'$ (the first derivative of $\mathfrak{S}$); $s_f''(x) = 1$ or 0 according as x belongs or does not belong to $\mathfrak{S}''$; and so on, till we reach $\mathfrak{S}^{(\beta)}$, no matter whether β belongs to the first or to the second class of numbers (cf. the definition in the Introduction of $s_f^{(\nu)}(x)$ for transfinite ν's). $g(x)$ is thus seen to have the required property.

By a slight modification of this example, we could retain the desired result, and, in addition, make $s_f^{(\beta)}(x) \not\equiv 0$.

We now prove the

THEOREM. *For every given function $g(x)$,† there exists a number β of the first or the second class, such that*

$$s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x) \equiv s_f^{(\beta+2)}(x) \equiv \cdots.$$

Proof. As in the case of the d-saltus, we see that $s_f''(x)$ is a nowhere-negative, upper-semi-continuous function, which is 0 in an everywhere dense set of points of (a, b). Let $\mathfrak{R}''$ denote the planar set of points whose coördinates are

$$x = x, \qquad y = s_f''(x) \quad (a \leqq x \leqq b);$$

more generally, $\mathfrak{R}^{(\beta)}$ (β = any number of the first or the second class), the planar set of points whose coördinates are

$$x = x, \qquad y = s_f^{(\beta)}(x) \quad (a \leqq x \leqq b).$$

Furthermore, let $\mathfrak{R}_d^{(\beta)}$ represent the set of points of $\mathfrak{R}^{(\beta)}$ that are points of denumerability of $\mathfrak{R}^{(\beta)}$; and $\mathfrak{R}_{nd}^{(\beta)}$, the points of $\mathfrak{R}^{(\beta)}$ that are points of non-denumerability of $\mathfrak{R}^{(\beta)}$. If $(\xi, s_f''(\xi))$ belongs to $\mathfrak{R}_{nd}''$, it follows, in virtue of the upper-semi-continuity of $s_f''(x)$, that $u_f(s_f'', \xi) = s_f''(\xi)$. Moreover, because $s_f''(x) \geqq 0$, and the zeros of $s_f''(x)$ are everywhere dense in (a, b), we have $l_f(s_f'', x) \equiv 0$. Therefore,

$$s_f'''(\xi) = u_f(s_f'', \xi) - l_f(s_f'', \xi) = s_f''(\xi)$$

if $(\xi, s_f''(\xi))$ belongs to $\mathfrak{R}_{nd}''$. This shows that every point of $\mathfrak{R}_{nd}''$ is also a point of $\mathfrak{R}'''$. But furthermore, every point of $\mathfrak{R}_{nd}''$ is also a point of

* The existence of such a set $\mathfrak{S}$ follows easily by means of finite and transfinite induction.

† Satisfying, of course, the conditions of uniqueness and boundedness demanded throughout.

$\mathfrak{R}_{nd}'''$. For according to a known theorem, $\mathfrak{R}_d''$ is at most a denumerable set. Hence $\mathfrak{R}'''$ and $\mathfrak{R}''$, coinciding in the points of $\mathfrak{R}_{nd}''$, differ at most in a denumerable set. The points of non-denumerability of $\mathfrak{R}''$ are thus also points of non-denumerability of $\mathfrak{R}'''$. Therefore, $\mathfrak{R}_{nd}''$ *is* actually *a subset of* $\mathfrak{R}_{nd}'''$.

Let us denote by $\mathfrak{A} \equiv \{\alpha_1, \alpha_2, \cdots\}$ the denumerable set of abscissas of the points of $\mathfrak{R}_d''$; and by $\mathfrak{B}$, the complementary set of abscissas of the points of $\mathfrak{R}_{nd}''$. Since $\mathfrak{R}_{nd}''$ is contained in $\mathfrak{R}_{nd}'''$, we have $s_f''(\xi) = s_f'''(\xi)$ for every ξ of $\mathfrak{B}$. Reasoning similar to that used above will show that $\mathfrak{R}_{nd}'''$ is contained in $\mathfrak{R}_{nd}^{\text{IV}}$, $\mathfrak{R}_{nd}^{\text{IV}}$ in $\mathfrak{R}_{nd}^{\text{V}}$, etc. Therefore, $\mathfrak{R}_{nd}''$ is contained in $\mathfrak{R}_{nd}^{(n)}$ for every finite $n > 2$; and hence $s_f''(\xi) = s_f^{(n)}(\xi)$ for every finite $n > 2$ and every ξ belonging to $\mathfrak{B}$. Accordingly, in virtue of our definition of $s_f^{(\nu)}(x)$ for transfinite ν (see Introduction), we conclude that $s_f''(\xi) = s_f^{(\omega)}(\xi)$, where ω is the first transfinite number. It is evident that the induction may be carried to every transfinite ordinal number of the second class.* Therefore, *for every* ξ *of* $\mathfrak{B}$ *and every number* $\nu > 2$ *of the first or the second class, we have* $s_f''(\xi) = s_f^{(\nu)}(\xi)$.

We thus see that the functions $s_f^{(\nu)}(x)$, where ν ($\geqq 2$) ranges over all the numbers of the first or the second class, differ at most on the lines $x = \alpha_n$ $\{n = 1, 2, \cdots\}$. We now show that these functions cannot all be different. For, if $s_f^{(\nu)}(\alpha_n) \neq s_f^{(\nu+1)}(\alpha_n)$, it follows from the fact that $s_f^{(\nu)}(x)$ is upper-semi-continuous, nowhere negative and equal to zero in an everywhere dense set, that $s_f^{(\nu+1)}(\alpha_n) < s_f^{(\nu)}(\alpha_n)$. Therefore, if $s_f^{(\nu+1)}(x) \not\equiv s_f^{(\nu)}(x)$, at least one of the points $(\alpha_n, s_f^{(\nu)}(\alpha_n))$ of $\mathfrak{R}^{(\nu)}$ must "slide" a finite distance toward the X-axis in order to reach coincidence with the corresponding point $(\alpha_n, s_f^{(\nu+1)}(\alpha_n))$ of $\mathfrak{R}^{(\nu+1)}$. That is to say, to every pair of different consecutive functions $\{s_f^{(\nu)}(x), s_f^{(\nu+1)}(x)\}$, there corresponds at least one interval on the lines $x = \alpha_n$ through which the "sliding" just referred to takes place. It is evident, on account of the monotone decrease of $s_f^{(\nu)}(x)$ with increasing ν, that two intervals corresponding to two different pairs of different consecutive functions may abut but never overlap. Hence the number of such intervals on each of the lines $x = \alpha_n$ is at most denumerable; and therefore the total number of such possible intervals is at most denumerable. Consequently, there

* The theorem that the limit of a sequence of monotone decreasing upper-semi-continuous functions is upper-semi-continuous is here utilized in passing to limiting numbers, such as ω, of the second class. The reader will readily verify (see also the next paragraph) that the sequence

$$s_f''(x), s_f'''(x), \cdots; s_f^{(\omega)}(x), s_f^{(\omega+1)}(x), \cdots; \cdots; \cdots s_f^{(\nu)}(x), s_f^{(\nu+1)}(x), \cdots; \cdots$$

is monotone decreasing; the theorem just referred to applies to subsequences of this sequence that have the ordinal type of the set of positive integers arranged in ascending magnitude.

cannot be more than a denumerable number of different pairs of different consecutive functions $s_f^{(\nu)}(x)$. If now the functions $s_f^{(\nu)}(x)$ were all different for all numbers $\nu \geqq 2$ of the first or the second class, there would be, contrary to the conclusion just reached, a non-denumerable infinity of pairs of different consecutive functions. Hence there must exist a number β of the first or the second class, such that $s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x)$, from which it follows that $s_f^{(\beta)}(x) \equiv s_f^{(\nu)}(x)$ for every $\nu > \beta$. Our proof is now complete.

We have shown above that if ξ belongs to $\mathfrak{B}$, then $s_f''(\xi) = s_f^{(\nu)}(\xi)$ for every $\nu > 2$ of the first or the second class. The converse also holds; namely, *if* $s_f''(\xi) = s_f^{(\nu)}(\xi)$ *for every* $\nu > 2$ *of the first or the second class, then* ξ *belongs to* $\mathfrak{B}$. This converse is a special case ($\lambda = 2$) of the following proposition:

If $(\xi, s_f^{(\lambda)}(\xi))$ *belongs to* $\mathfrak{R}_d^{(\lambda)}$, *where* $\lambda \geqq 2$ *is a number of the first or the second class, then for some number* μ *of the first or the second class* $> \lambda$, *we have*

$$s_f^{(\lambda)}(\xi) > s_f^{(\mu)}(\xi).$$

For suppose that, contrary to the conclusion of this proposition, it were true that $s_f^{(\nu)}(\xi) = s_f^{(\lambda)}(\xi)$ for every ν of the first or the second class $> \lambda$. It would then follow, in virtue of the upper-semi-continuity of $s_f^{(\nu)}(x)$ and its monotone decrease with increasing ν, that $(\xi, s_f^{(\nu)}(\xi))$ belonged to $\mathfrak{R}_d^{(\nu)}$ for every ν of the first or the second class $> \lambda$. This is, however, impossible, on account of the following theorem and the fact shown above that for some β of the first or the second class $s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x)$.

THEOREM. *The relation* $s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x)$ *implies that every point* $(\xi, s_f^{(\beta)}(\xi))$ *belongs to* $\mathfrak{R}_{nd}^{(\beta)}$.

Proof. Suppose that $\mathfrak{R}_d^{(\beta)}$ were not the null-set, and the point

$$P \equiv (\xi, s_f^{(\beta)}(\xi)) \equiv (\xi, \eta)$$

an element of it. Then, in virtue of the upper-semi-continuity of $s_f^{(\beta)}(x)$ and the fact that P belongs to $\mathfrak{R}_d^{(\beta)}$, it is possible to enclose P in a region

$$R\colon\ \xi - \delta \leqq x \leqq \xi + \delta, \qquad y \geqq \eta - \delta \quad (\delta > 0),$$

such that R contains in its interior and on its boundary no more than a denumerable set of points of $\mathfrak{R}^{(\beta)}$. Moreover, we may and we do assume, that there is no point of $\mathfrak{R}^{(\beta)}$ on the boundary of R; if originally R possesses such points, we may evidently select from the continuum of similar regions

$$R'\colon\ \xi - \delta' \leqq x \leqq \xi + \delta', \qquad y \geqq \eta - \delta' \quad (\delta > \delta' > 0)$$

one having on its boundary none of the denumerable points of $\mathfrak{R}^{(\beta)}$ situated in R. Let $\mathfrak{C}$ represent the set of abscissas of points of $\mathfrak{R}^{(\beta)}$ that lie in R. I say that $\mathfrak{C}$ is closed. For suppose that $\{\gamma_n\}$, $n = 1, 2, \cdots$, is a sequence of elements of $\mathfrak{C}$ having γ as a limit. Then the points $(\gamma_n, s_f^{(\beta)}(\gamma_n))$ are all in R. We wish to show that $(\gamma, s_f^{(\beta)}(\gamma))$ is also in R. From the sequence of points $(\gamma_n, s_f^{(\beta)}(\gamma_n))$, a subsequence $(\gamma_{m_n}, s_f^{(\beta)}(\gamma_{m_n}))$ may be extracted having as limit a single point (γ, k), say, lying in the interior or on the boundary of R. Since $s_f^{(\beta)}(x)$ is upper-semi-continuous, it must be that $s_f^{(\beta)}(\gamma) \geqq k$. Therefore, $(\gamma, s_f^{(\beta)}(\gamma))$ is not below (γ, k), and hence, in R. $\mathfrak{C}$ is thus closed. Being, furthermore, denumerable, it must be reducible, and it therefore contains at least one isolated value, say $\bar{\gamma}$. A fortiori, the point $(\bar{\gamma}, s_f^{(\beta)}(\bar{\gamma}))$, being an interior point of R, is an isolated point of $\mathfrak{R}^{(\beta)}$; and therefore, because of the upper-semi-continuity of $s_f^{(\beta)}(x)$ and the everywhere dense distribution of its zeros, we have

$$s_f^{(\beta+1)}(\bar{\gamma}) < s_f^{(\beta)}(\bar{\gamma}).$$

Therefore, if $\mathfrak{R}_d^{(\beta)}$ is not the null-set, $s_f^{(\beta+1)}(x) \not\equiv s_f^{(\beta)}(x)$.

From the above considerations, we may deduce the following interesting connection between the d-saltus and the f-saltus.

THEOREM. *For every function $g(x)$, for which $s_f^{(\beta)}(x) \equiv s_f^{(\beta+1)}(x)$, we have*

$$s_d(s_f'', x) \equiv s_f^{(\beta)}(x).$$

For the proof, further details of which are left to the reader, we note that $(\xi, s_f^{(\beta)}(\xi))$ is the highest point of non-denumerability of $\mathfrak{R}''$—of course, not necessarily belonging to $\mathfrak{R}''$—on the line $x = \xi$.

5. The e-saltus. THEOREM. $s_e'''(x) \equiv 0$.

Proof. Just as in the previous two cases, it is seen that $s_e''(x) = 0$ at the points of continuity of $s_e'(x)$. Since the points of discontinuity of $s_e'(x)$ constitute an exhaustible set $\mathfrak{S}$,* we have $s_e''(x) = 0$ everywhere except possibly in $\mathfrak{S}$. The values of $s_e''(x)$ in $\mathfrak{S}$ may be neglected when $s_e'''(x)$ is calculated. Hence $s_e'''(x) = 0$.

The following example shows that $s_e''(x)$ need not equal $s_e'''(x)$. Let $(a, b) \equiv (0, 1)$, and let $\mathfrak{M}_1$ and $\mathfrak{M}_2$ be two complementary sets of the interval $(0, \frac{1}{2})$, such that both $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are inexhaustible (i. e., of second category) in every subinterval of $(0, \frac{1}{2})$.† Let $g(x) = 0$ if x belongs to $\mathfrak{M}_1$, and $g(x) = 1$ if x does not belong to $\mathfrak{M}_1$. Then

* See, for example, Hobson, l. c., p. 244.

† For the existence of such complementary sets, see the example of Mahlo in Schoenflies-Hahn, *Entwickelung der Mengenlehre und ihrer Anwendungen* (1913), p. 349. The example is on Zermelo's "*Auswahlpostulat.*"

$$s_e'(x) = 1 \quad (0 \leqq x \leqq \tfrac{1}{2}), \qquad s_e'(x) = 0 \quad (\tfrac{1}{2} < x \leqq 1);$$

$$s_e''(x) = 0 \quad (x \neq \tfrac{1}{2}), \qquad s_e''(\tfrac{1}{2}) = 1; \qquad s_e'''(x) \equiv 0.$$

Remark. *If* $s_i'(x)$, $s_i''(x)$, $s_i'''(x)$, $\cdots$ *represent the successive saltus functions that arise when,* instead of neglecting exhaustible sets, *we neglect nowhere-dense sets, then* $s_i'''(x) \equiv 0$. For, as in the case of the e-saltus, we show that $s_i''(x)$ is 0 everywhere except in an exhaustible set. Let $\{\epsilon_n\}$ be a sequence of positive numbers such that $\lim_{n\to\infty} \epsilon_n = 0$; and let $\mathfrak{C}_n$ be the set of abscissas x at which $s_i''(x) \geqq \epsilon_n$. Then $\mathfrak{C}_n$ is a nowhere-dense set.* $\mathfrak{C}_n$ may therefore be neglected in the calculation of $s_i'''(x)$. For the remaining points of (a, b), we have $s_i''(x) < \epsilon_n$. This inequality, holding for every n, shows that $s_i'''(x) \equiv 0$.

6. The z-saltus. THEOREM. $s_z'''(x) \equiv s_z^{\text{IV}}(x) \equiv s_z^{\text{V}}(x) \equiv \cdots$.

The proof proceeds along the same lines as that of the corresponding theorem of § 3.† We shall, however, make clear how the parallelism is effected.

As in the previous cases, we see that $s_z''(x)$ is a nowhere negative, upper-semi-continuous function, whose zeros are everywhere dense in (a, b). Let (α, β) be any subinterval of (a, b) and γ a point in the interior of (α, β) for which $s_z''(\gamma) = 0$. Since $s_z''(x)$ is upper-semi-continuous, there exists, for every $\epsilon > 0$, a subinterval $(\gamma - \delta, \gamma + \delta)$ of (α, β) throughout which $s_z''(x) < \epsilon$. Therefore, no matter what set of zero measure is neglected, there still remain points in $(\gamma - \delta, \gamma + \delta)$ at which $s_z''(x) < \epsilon$. This shows that $l_z(s_z'', \alpha\beta) < \epsilon$ for every subinterval (α, β) and every $\epsilon > 0$. Therefore, for every x,

$$l_z(s_z'', x) = 0,$$

and

$$s_z'''(x) = u_z(s_z'', x) - l_z(s_z'', x) = u_z(s_z'', x) \leqq s_z''(x).$$

Now let $\mathfrak{R}''$ be the planar set of points whose coördinates are $x = x$, $y = s_z''(x)$ $(a \leqq x \leqq b)$. If P is any point of the plane, whether belonging to $\mathfrak{R}''$ or not, there are two mutually exclusive possibilities: (1) There exists a neighborhood of P such that the projection upon the X-axis of the set of points of $\mathfrak{R}''$ in it is a set of measure 0. (2) Every neighborhood of P contains a set of points of $\mathfrak{R}''$ whose projection upon the X-axis is not a set of measure 0.‡ In the first case, we shall say that P is a "*z-point*" of $\mathfrak{R}''$; in the second case, that P is a "*$\bar{z}$-point*" of $\mathfrak{R}''$.

* Cf., for example, Hobson, l. c., pp. 243 and 244.

† It would be easy to set up, on the basis of a suitable system of postulates, a theory having as consequence a common generalization of the theorem of the present section and of that in § 3. Cf. E. H. Moore, Introduction to a Form of General Analysis (1910), p. 1. Cf. also Appendix.

‡ The projection is then either of measure > 0 or non-measurable.

Just as in the case of the d-saltus, we may now show that *for every* ξ *of* (a, b), *the point* $(\xi, s_z'''(\xi))$ *is the highest* $\bar{z}$*-point of* $\mathfrak{R}''$ *on the line* $x = \xi$. All we have to do is to substitute, in the proof of the corresponding statement of § 3, "z-point" for "point of denumerability," "$\bar{z}$-point" for "point of non-denumerability," "set of points whose projection on the X-axis is of zero measure" for "denumerable set," s_z'' for s_d'', etc. In particular, it follows, as there, that if $(\xi, s_z''(\xi))$ is itself a $\bar{z}$-point of $\mathfrak{R}''$, then $s_z'''(\xi) = s_z''(\xi)$.

To complete the proof in the analogous fashion intended, it will now be seen that all we need is the analogue of the theorem in § 3, that the points of denumerability of $\mathfrak{R}''$ constitute at most a denumerable set; namely, the theorem, that the projection upon the X-axis of the set of z-points of $\mathfrak{R}''$ is a set of zero measure. This may be easily proved as follows. Divide the plane into squares by means of the lines $x = \pm n/2^k$, $y = \pm n/2^k$, where $n = 0, 1, 2, \cdots$, and k is a positive integer. For a fixed k, we get a single system of squares. Letting $k = 1, 2, 3, \cdots$, we obtain a denumerable set of systems of squares. Let us call the square S a "*z-square,*" if it belongs to any one of these systems and is furthermore such that the projection upon the X-axis of the set of points of $\mathfrak{R}''$ in the interior or on the boundary of S is a set of zero measure. Since the number of "z-squares" is denumerable, the projection upon the X-axis of the totality of points of $\mathfrak{R}''$ in the interior or on the boundary of all the "z-squares" must be a set of zero measure; for the measure of a set of denumerable sets is the sum of the measures of these sets. But, as may be readily seen from the definition of "z-point" and of "z-square," every z-point is in the interior or on the boundary of at least one z-square. Hence, the projection of the totality of z-points of $\mathfrak{R}''$ is of zero measure, and our theorem is proved.

The following example shows that $s_z''(x)$ need not equal $s_z'''(x)$. Let $(a, b) \equiv (0, 1)$ and let $\mathfrak{M}_1$ and $\mathfrak{M}_2$ be two complementary sets of the interval $(0, \frac{1}{2})$ such that in every subinterval of $(0, \frac{1}{2})$ both $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are either non-measurable or of measure > 0.* Let $g(x) = 0$, if x belongs to $\mathfrak{M}_1$, and $g(x) = 1$, if x does not belong to $\mathfrak{M}_1$. Then

$$s_z'(x) = 1 \quad (0 \leqq x \leqq \tfrac{1}{2}), \qquad s_z'(x) = 0 \quad (\tfrac{1}{2} < x \leqq 1);$$

$$s_z''(x) = 0 \quad (x \neq \tfrac{1}{2}), \qquad s_z''(\tfrac{1}{2}) = 1; \qquad s_z'''(x) \equiv 0.$$

Remark. An *apparently* different type of saltus may be defined as follows. If (α, β) is any subinterval of (a, b), let $s_\epsilon(g, \alpha\beta)$ be the saltus

* For the existence of such complementary sets, see Schoenflies-Hahn, l. c., pp. 374–378, where examples showing the required existence, constructed by Vitali, Lebesgue, Van Vleck and Hausdorff, are described. All these examples are based on Zermelo's "*Auswahlpostulat.*"

of $g(x)$ in (α, β), if sets of measure ϵ—or of measure $\epsilon/(\beta - \alpha)$—may be neglected. (Cf. the definitions given in the Introduction.) As ϵ decreases, $s_\epsilon(g, \alpha\beta)$ surely does not decrease; and therefore, since $g(x)$ is bounded, $s_\epsilon(g, \alpha\beta)$ has a definite limit for $\epsilon \to 0$, which we may denote by $s_{\epsilon \to 0}(g, \alpha\beta)$. It is readily seen, however, that $s_{\epsilon \to 0}(g, \alpha\beta)$ is identical with our $s_z(g, \alpha\beta)$.

Appendix—Remarks on Generalizations.

Throughout our discussion so far, we have dealt with a real function $g(x)$, defined in an interval (a, b) and further restricted to being single-valued and bounded. In fact, however, our results are essentially far more general. It is not difficult to see how most of our definitions and proofs may be extended to the case of many-valued, bounded or unbounded functions of several variables, or of infinitely many variables. But even such an extension would be short of the full intrinsic generality of our considerations. The reader cannot have failed to notice that throughout the discussion, only a small number of basal notions and properties were utilized. To indicate, if but vaguely, the degree to which the generalization of some of our results may be carried, we refer to a paper, read by the author before the American Mathematical Society.* In this paper, it was shown how several of the theorems in the present paper, and others closely related, may be proved for a "neighborhood" theory of a class $\mathfrak{R}$, in which the main assumption—there are other postulates playing a minor rôle—is approximately as follows: If $\mathfrak{N}_1$ and $\mathfrak{N}_2$ are both neighborhoods of the element P of $\mathfrak{R}$, then there exists a neighborhood of P contained in both $\mathfrak{N}_1$ and $\mathfrak{N}_2$. The publication of the suggested generalization of our present results is, however, reserved for the future.

* See notice in Bulletin of the American Mathematical Society, March, 1915, p. 289.

UNIVERSITY OF NEBRASKA,
October 20, 1916.

FERMAT'S LAST THEOREM AND THE ORIGIN AND NATURE OF THE THEORY OF ALGEBRAIC NUMBERS.

By L. E. Dickson.

Introduction.

Of the many interesting and important facts about whole numbers which were discovered by Fermat nearly three centuries ago, all have since been proved with one exception, the so-called last theorem of Fermat, which asserts that $x^n + y^n = z^n$ has no integral solutions different from zero when $n > 2$. Fermat stated that he had found a truly remarkable proof. His scientific reputation is such that one can at most doubt the accuracy of his proof. This challenge problem has received attention from many mathematicians of the highest ability, including Euler, Legendre, Gauss, Abel, Sophie Germain, Dirichlet, Kummer and Cauchy.

The problem is important chiefly on account of its relation to the history of mathematics. The publication of a complete proof would deprive the problem of its chief claim to attention for its own sake, but not its claim to historical importance. For, the study of this challenge problem and the general law of reciprocity of higher residues led Kummer to invent his ideal numbers, out of which grew the general theory of algebraic numbers, one of the most important branches of modern mathematics. As remarked by Hensel,* it would seem at first sight to be a misfortune that Fermat did not have space on the margin of his copy of Diophantus to write down his proof; but further reflection leads one to regard this circumstance as one fortunate for the development of science; for, while we might perhaps have possessed a complete proof of Fermat's theorem, not in itself so important, we would certainly not possess Kummer's ideal theory which grew up solely out of attempts to prove that theorem. Kummer devoted twenty of his best years to the development of his ideal numbers, holding always before himself as goal the complete proof of Fermat's last theorem and the general reciprocity law, and declaring that he would probably have abandoned his theory of ideal numbers, in spite of its success, if he had known another method of proving that theorem and law. We, to whom Kummer's theory appears

* Abhand. Geschichte Math. Wiss., 29, 1910, p. 19, p. 30.

as the foundation stone of arithmetic, are of another opinion; we would on the contrary thank Fermat's problem that through it the genius of a Kummer was so forcibly directed that we now possess the theory of ideals. Gauss had previously investigated the special algebraic integers $a + bi$ in connection with the law of reciprocity of biquadratic residues.

Part I of this paper is devoted to the early history of Fermat's last theorem and to a summary of the more important results concerning it which have been proved without the theory of algebraic numbers. The papers which treat Fermat's theorem by means of algebraic numbers are reserved for Part III. The points of view needed for this final part are developed in a very elementary way in Part II.

But the chief aim of Part II (which may be read independently of Parts I and III) is to enable the general reader to obtain, with a minimum of effort, a clear insight into the origin, nature and use of ideals. The exposition is limited to the concrete, but typical, case of a particular quadratic domain, thereby avoiding the algebraic complications which arise for the general domain.

Contrary to the intuition of Lamé, Cauchy, Wantzel and initially of Kummer himself, the numbers involving a single algebraic irrationality do not obey the laws of arithmetic; the restoration of those laws by the introduction of the ideals was one of the chief scientific triumphs of the last century.

The writer is indebted to H. S. Vandiver and H. H. Mitchell for suggestions on the manuscript and proof sheets.

Part I.

Early History of Fermat's Last Theorem. Results Obtained Without the Use of the Theory of Ideals.

1. Sum of two cubes not a cube. A defective proof was given before 972 by the Arab Alkhodjandi.* The Arab Beha-eddin† (1547–1622) listed among the problems remaining unsolved from former times that to divide a cube into two cubes. P. Fermat‡ proposed the problem to find two cubes whose sum is a cube to Sainte-Croix, September, 1636, to Frenicle, May, 1640, to the mathematicians of England and Holland, August 15, 1657, and later§ declared that the problem is impossible.

* Cf. F. Woepcke, Atti Accad. Pont. Nuovi Lincei, 14, 1866–1, 301.

† Essenz der Rechenkunst von Mohammed Beha-eddin ben Alhossain . . . von G. H. F. Nesselmann, 1843, p. 55. French transl. by A. Marre, Nouv. Ann. Math., 5, 1846, 313; ed. 2, Rome, 1864.

‡ Oeuvres de Fermat, 2, p. 65, p. 195, p. 346; 3, p. 287, p. 313.

§ Oeuvres, 2, p. 376, p. 433, letter to Digby, Apr. 7, 1658, to Carcavi, Aug., 1659.

The proof by Euler* was reproduced by Legendre.† Gauss‡ gave a proof by use of a cube root of unity.

2. **Sum or difference of two biquadrates never a square.** Each of these propositions implies that $x^4 + y^4 = z^4$ is impossible in integers not zero. Leonardo Pisano§ gave an incomplete proof of the fact that $x^2 + y^2$ and $x^2 - y^2$ are not both squares and implied the related theorem that the area of a right triangle with rational sides is never a perfect square. P. Fermat's‖ proof of the latter theorem is of special interest as it illustrates his famous method of infinite descent and as it is the only instance of a detailed proof left by him. The proof shows incidentally that the difference of two biquadrates is not a square. An analogous proof, doubtless due to Fermat, was published by Frenicle de Bessy,¶ who proved also that no square is a sum of two biquadrates. In a MS. dated Dec. 29, 1678, Leibniz** proved that the area of a primitive right triangle with integral sides is not a square; hence $v^4 - w^4$ is not a square, as shown by the area of the triangle formed from v^2 and w^2 by Diophantus's rule.†† Euler‡‡ gave simple proofs that $a^4 + b^4 \neq c^2$ if $ab \neq 0$; $a^4 - b^4 \neq c^2$ if $b \neq 0, b \neq a$; these proofs were reproduced by Legendre.§§

3. **Fermat's theorem from elementary standpoints.** About 1637, P. Fermat,‖‖ commenting on Diophantus II, 8 (to solve $x^2 + y^2 = a^2$), stated that "it is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into two powers of like degree; I have discovered a truly remarkable proof which this margin is too small to contain."

Claude Jaquemet¶¶ (1651–1729) gave a false proof, thinking that

* Algebra, 2, 1770, art. 243, pp. 509–16; French tr., 1774, 2, pp. 343–51; Opera Omnia (1), 1, 484–9.

† Théorie des nombres, 1798, pp. 407–8. Cf. ed. 3, 1830, art. 653.

‡ Posthumous MS., Werke, 2, 387–390.

§ Tre Scritte Inediti de L. Pisano, Rome, 1854, p. 98. Scritti di L. Pisano, Rome, vol. 2, 1862, p. 272. Cf. Genocchi, Annali di Sc. Mat. Fis., 6, 1855, 131–2, 293–310.

‖ Fermat's marginal notes on his copy of Bachet's edition (1621) of Diophantus's Arithmetica. Oeuvres de Fermat, 1, 1891, p. 340; 3, 1896, p. 271.

¶ Traité des Triangles Rectangles en Nombres, Paris, 1676, pp. 101–6; Mém. Acad. Sc. Paris, 1666–1699, p. 5, éd. 1729, p. 178.

** Math. Schriften (ed. C. I. Gerhardt), vol. 7, 1863, pp. 120–5.

†† The triangle formed from m, n has the sides $2mn$, $m^2 - n^2$, $m^2 + n^2$.

‡‡ Comm. Acad. Petrop., 10, 1747 (1738), pp. 125–134; Comm. Arith. Coll., 1, pp. 24–34. Same in Euler's Algebra, 2, 1770, p. 418; 1774, pp. 242–54; Opera omnia (1), 1, 1911, p. 437.

§§ Théorie des nombres, 1798, p. 404; ed. 2, 1808; Maser, 1893, 2, p. 5.

‖‖ Diophanti Alexandri Arith. libri sex, ed. S. Fermat, Tolosæ, 1670, p. 61. Oeuvres de P. Fermat, 1, p. 291; 3, p. 241.

¶¶ Ms. in the Bibliothèque Nationale de Paris, published by A. Marre, Bull. Bibl. Storia Sc. Mat. Fis., 12, 1879, 886–894. Cf., pp. 565–8.

$p - r$ cannot divide $pq - rs$. Sophie Germain,* in her first letter to Gauss, Nov. 21, 1804, stated that she could prove that

$$[1] \qquad x^n + y^n + z^n = 0$$

is impossible if $n + 1$ is a prime of the form $8k + 7$.

P. Barlow† considered integers x, y, z relatively prime in pairs, each not zero, and satisfying [1], where n is an odd prime. Then

$$[2] \qquad \phi(x, y) = \frac{x^n + y^n}{x + y} = x^{n-1} - x^{n-2}y + \cdots + y^{n-1}$$

is either prime to $x + y$ or has with it the greatest common divisor n, according as z is not or is divisible by n, a result due to Jacquemet. In the respective cases, Barlow deduced [4] and [5]. His attempt to prove the impossibility of [1] involved the error that a sum of fractions in their lowest terms is not an integer if the denominator of each fraction has a factor not dividing all the remaining denominators.

N. H. Abel‡ stated that solutions of [1] are of the form [4], [5] or

$$2x = c^n + n^{n-1}(a^n + b^n), \qquad 2y = c^n - n^{n-1}(a^n + b^n),$$
$$2z = -c^n - n^{n-1}(a^n - b^n).$$

But the third case is unnecessary. He stated that [1] is impossible when any of the quantities $x, y, z, x - y, x - z, y - z, x^{1/n}, y^{1/n}, z^{1/n}$ are primes.

A. M. Legendre,§ after remarking that the French Academy of Sciences had offered one of its prizes for a proof of Fermat's last theorem, but without awarding the prize, developed some results which he credited to Sophie Germain. First, let no one of the relatively prime numbers x, y, z satisfying [1] be divisible by the odd prime n. Then $x + y$ and the expression [2] are relatively prime and their product equals $(-z)^n$. Hence we may set

$$[3] \qquad \begin{array}{lll} y + z = a^n, & \phi(y, z) = \alpha^n, & x = -a\alpha, \\ z + x = b^n, & \phi(z, x) = \beta^n, & y = -b\beta, \\ x + y = c^n, & \phi(x, y) = \gamma^n, & z = -c\gamma. \end{array}$$

* Oeuvres phil., 1879, p. 298. Cinq lettres de S. Germain à Gauss, 1880. Archiv Math. Phys., 65, 1880, Litt. Bericht, pp. 27–31.

† Appendix to English transl. of Euler's Algebra. Proof "completed" in Jour. Nat. Phil. Chem. Arts, 27, 1810, p. 193 and reproduced in Barlow's Theory of Numbers, London, 1811, 166–9. Changing the sign of x, we shall write his equation in the form [1].

‡ Oeuvres, 2, 1881, 254–5, letter to Holmboe, Aug. 3, 1823.

§ Mém. Ac. R. Sc. de l'Institut de France, 6, année 1823, Paris, 1827, pp. 1–60. Reproduced in his Théorie des nombres, ed. 2, second supplément, Sept., 1825, pp. 1–40.

Thus

[4] $2x = b^n + c^n - a^n, \qquad 2y = a^n + c^n - b^n, \qquad 2z = a^n + b^n - c^n.$

Second, let x be divisible by n; we obtain results like [3] including

[5] $$y + z = n^{n-1}A^n, \qquad z + x = b^n, \qquad x + y = c^n.$$

To Sophie Germain is credited the ingenious and important theorem that *if there exists an odd prime p such that*

[6] $$\xi^n + \eta^n + \zeta^n \equiv 0 \pmod{p}$$

has no set of integral solutions ξ, η, ζ, each not divisible by p, and if n is not the residue modulo p of the nth power of any integer, then [1] *has no integral solutions each prime to n.* For, such solutions satisfy also congruence [6], so that one of them, say x, is divisible by p, whence, by [4],

$$b^n + c^n + (-a)^n \equiv 0 \pmod{p}.$$

Hence a, b or c is divisible by p. But, if b were divisible by p, then, by [3], $y = -b\beta$ would be divisible by p, and hence by [1] also z would be divisible by p, whereas x, y, z have no common factor. Similarly, c is not divisible by p. Hence

$$a \equiv 0, \qquad x \equiv 0, \qquad z \equiv -y,$$

$$\phi(x, y) \equiv y^{n-1}, \qquad \phi(y, z) \equiv ny^{n-1} \pmod{p}.$$

Thus, by [3], $\gamma^n \equiv y^{n-1}$, $\alpha^n \equiv ny^{n-1}$, whence $n\gamma^n \equiv \alpha^n \pmod{p}$. By the final equation [3], γ is prime to p. Hence we can determine an integer t such that $\gamma t \equiv 1 \pmod{p}$. Thus $n \equiv (\alpha t)^n \pmod{p}$, contrary to hypothesis.

The conditions in the theorem are satisfied if $n = 7$, $p = 29$, since the residues of the seventh powers of all integers modulo 29 are ± 1, ± 12, no two of which differ by unity, and since no one of these residues is congruent to 7. Likewise, for each odd prime $n < 100$, S. Germain gave a prime p for which the theorem applies, and hence concluded that Fermat's equation [1] has no integral solutions each prime to n, when $2 < n < 100$.

The condition that n shall not be a residue of an nth power requires that the prime modulus p be of the form $mn + 1$, where m is even since p is odd. Legendre proved (§§ 23–28) that m must be prime to 3 and that both of the conditions in the theorem hold if $p = mn + 1$ is a prime and $m = 2, 4, 8, 10, 14, 16$, but overlooked the exceptional character of $n = 3$ when $m = 14$ or 16. He concluded that [1] has no solutions prime to n if $2 < n < 197$.

Legendre proved (§§ 38–47) that $x^5 + y^5 + z^5 = 0$ has no integral solutions. Dirichlet had already presented to the Paris Academy, July 11, 1825, a proof for the case in which z is even, if z is the unknown divisible by 5, and soon published* a proof by a method applying as well to the case z odd, whereas Legendre had treated the two cases by two methods. Dirichlet† proved by the method of descent that [1] is impossible if $n = 14$.

G. Libri‡ proved for $n = 3$ and $n = 4$ and stated for any n that for the primes p, exceeding an assignable limit, congruence [6] has solutions prime to p, so that it is futile to attempt to prove Fermat's theorem by trying to show that one of the unknowns is divisible by an infinitude of primes.

G. Lamé§ proved Fermat's theorem for the exponent 7. Simplifications were made by V. A. Lebesgue‖ and A. Genocchi.¶ The latter** gave the generalization that there is no solution such that x, y, z are the roots of a cubic equation with rational coefficients. T. Pepin†† gave another proof of Lamé's result and that of Libri for $n = 3$.

In 1883 the Belgian Academy of Sciences offered a prize for a proof of Fermat's last theorem; no award was made.

A. E. Pellet‡‡ found by means of inequalities in the theory of roots of unity that congruence [6], for a prime modulus $p = n\omega + 1$, has solutions each not divisible by p for every ω exceeding a certain limit (not specified) for which $n\omega + 1$ is a prime. This is the essential part of Libri's assertion quoted above.

E. Wendt§§ noted that, if n and $p = mn + 1$ are odd primes, congruence [6] has no solutions ξ, η, ζ, each prime to p, if and only if p is not a divisor of the resultant D_m of

$$[7] \qquad z^m \equiv 1, \qquad (z+1)^m \equiv 1 \pmod{p}.$$

For, if ω is determined by $\omega\zeta \equiv 1 \pmod{p}$, the product of [6] by ω^n gives a congruence of the form $z + 1 \equiv y \pmod{p}$, where z and y are nth powers,

* Jour. für Math., 3, 1828, 354–375; Werke, 1, 1–46.

† Ibid., 9, 1832, 390–3; Werke, 1, 189–194.

‡ Ibid., pp. 270–5.

§ Comptes Rendus, Paris, 9, 1839, 45–6; Mém. prés. divers savants ac. sc. Institut France, 8, 1843, 421–37. Jour. de Math., 5, 1840, 195–211 (pp. 211–5 for report by Cauchy; Oeuvres (1), 4, 499).

‖ Jour. de Math., 5, 1840, 276–9, 348–9.

¶ Annali di mat., 6, 1864, 287–8.

** Comptes Rendus, Paris, 78, 1874, 435; 82, 1876, 910–3.

†† Ibid., 82, 1876, 676–9; 91, 1880, 366–8.

‡‡ Bull. Soc. Math. France, 15, 1886–7, 93.

§§ Jour. für Math., 113, 1894, 335–347.

so that their mth powers are congruent to unity by Fermat's lesser theorem. Hence S. Germain's theorem may be expressed as follows: If $mn + 1$ is a prime dividing neither $n^m - 1$ nor

$$D_m = \begin{vmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-1} \\ \binom{m}{m-1} & 1 & \binom{m}{1} & \cdots & \binom{m}{m-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{m}{1} & \binom{m}{2} & \binom{m}{3} & \cdots & 1 \end{vmatrix},$$

Fermat's equation for the prime exponent $n > 2$ is impossible in integers all prime to n. The same conclusion follows if $m = 2^\nu n^k$ can be so chosen that $mn + 1$ is a prime not dividing D_m, where ν is not divisible by the prime n.

Dickson* noted that, if a is a common root of congruences [7],

$$a, \quad \frac{1}{a}, \quad -1-a, \quad \frac{1}{-1-a}, \quad -1-\frac{1}{a}, \quad \frac{-a}{1+a}$$

are common roots and are distinct if $2^m - 1$ is not divisible by p. They are the roots of a sextic in z which is unaltered when z is replaced by $1/z$ or by $-1-z$. The sextic must divide $z^m - 1$ modulo p. Set $x = z + 1/z$, $m = 2\mu$. The sextic becomes

$$C(x) = x^3 + 3x^2 + \beta x + 2\beta - 5.$$

From $z^\mu - 1/z^\mu = 0$ we get $f(x^2) = 0$, where $f(\omega)$ is of degree $\frac{1}{2}\mu - 1$ or $(\mu - 1)/2$ according as μ is even or odd. Thus $f(x^2)$ must be divisible by $S(x) = C(x)C(-x) = x^6 + (2\beta - 9)x^4 + (\beta^2 - 12\beta + 30)x^2 - (2\beta - 5)^2$. Hence $\mu \geqq 7$. For $\mu = 7$, $f(x^2) = x^6 - 5x^4 + 6x^2 - 1$ must be congruent to $S(x)$, whence $p = 2$. For $\mu = 8$, $f(x^2) = x^6 - 6x^4 + 10x^2 - 4$, whence $p = 17$, contrary to $n > 1$. The cases $\mu = 10, 11, 13$ are readily treated. The conclusion is that, if n and $p = mn + 1$ are odd primes, m being prime to 3 and $m \leqq 26$, congruence [6] has no integral solutions each prime to p, except for $n = 3$, $m = 10, 14, 20, 22, 26$; $n = 5$, $m = 26$; $n = 31$, $m = 22$. A direct examination of [7] was made for $m = 28, 32, 40, 56, 64$. By use of these results and the theorem of S. Germain, it was shown that Fermat's equation is impossible in integers prime to n for every odd prime exponent $n < 1700$.

Dickson† proved the last result for $n < 7000$ by extending the range of the m's to include all values < 74, as well as 76 and 128.

* Messenger of Math. (2), 38, 1908, 14–32.

† Quart. Jour. Math.. 40, 1908, 27–45. The case 6857 was excluded later.

Dickson* proved, by use of Jacobi's functions of roots of unity, that if n and p are odd primes such that

$$p \equiv (n-1)^2(n-2)^2 + 6n - 2,$$

congruence [6] has integral solutions each prime to p, thus establishing independently of Pellet the conjecture by Libri in 1832. G. Cornacchia† obtained a like result by the same methods.

It is perhaps superfluous to mention the bequest by P. Wolfskehl to the K. Gesellschaft des Wissenschaften of Göttingen as a prize for a complete proof of Fermat's last theorem.

A. Fleck‡ considered the common factors of the six functions $x^2 + xy + y^2, \cdots, z^2 - xy$ of solutions of Fermat's equation [1].

B. Lind§ gave an account of numerous papers not employing algebraic numbers; of the results claimed as novel, the earlier ones are well known and the later ones erroneous.

A. Pellet|| proved by use of the equation for the n periods of the pth roots of unity, where $p = hn + 1$ is a prime, that congruence [6] has solutions not divisible by p if $h^4 > (p-h)^3$, which he stated erroneously to follow from $h > n\sqrt{n}$ [the latter, but not the former, holds if $n = 5$, $h = 20$].

Part II.

The Origin of the Theory of Algebraic Numbers

4. Erroneous views on algebraic numbers prevalent in 1847. G. Lamé¶ attempted to prove that Fermat's equation for any odd prime exponent n is not satisfied by complex integers

$$[8] \qquad a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

where α is an imaginary nth root of unity, and the a's are integers. As pointed out by Liouville (ibid., pp. 315–6), Lamé had not shown that a complex integer is decomposable into complex primes in a single manner. Lamé (p. 352) admitted this lacuna in his proof, but believed (on the basis of extensive tables of factorizations) that it could be filled, affirming (p. 569, p. 888) that the ordinary laws for integers hold for complex integers when $n = 5$. Lamé** presented his arguments in two long memoirs.

* Jour. für Math., 135, 1909, 181–8. Cf. Hurwitz, 136, 1909, 272–292.
† Giornale di mat., 47, 1909, 219–268.
‡ Sitzungs. Berliner Math. Gesell., 8, 1909, 133–148; 9, 1910, 50–3.
§ Abh. Geschichte Math. Wiss., 26, II, 1910, 23–65.
|| L'intermédiaire des math., 18, 1911, 81–2.
¶ Comptes Rendus, Paris, 24, 1847, 310–5.
** Jour. de math., 12, 1847, 137–171, 172–184.

E. E. Kummer* pointed out the falsity of Lamé's assumption that every complex integer [8] can be decomposed into primes in a single way. It is an instructive fact that Kummer himself made the same false assumption a short time before in constructing what he then believed to be a complete proof of Fermat's theorem.† The MS. was submitted to Dirichlet, who declared the proof would be as correct as it was elegant if Kummer had proved not merely that every number [8] can be factored into indecomposable numbers, but also that this factorization is possible in only one way, and expressed his belief that unfortunately the numbers [8] do not in general possess this property.

Wantzel‡ proved that Euclid's greatest common divisor process holds for complex integers $a + b\sqrt{-1}$ (as Gauss had shown) and for complex integers $a + b\omega + c\omega^2$ formed from an imaginary cube root ω of unity, and stated that a like property holds for complex integers [8], with n arbitrary, since the norm of [8] is less than unity when $a_0, \cdots, a_{n-1}$ are between 0 and 1. Here the norm of [8] means the product of [8] by the complex numbers obtained from it by replacing α by the remaining primitive nth roots of unity. A. Cauchy§ showed that this statement that the norm is < 1 is false for $n = 7$ and for any prime $n = 4m + 1 \geqq 17$, and pointed out lacunæ in Lamé's proof.

Cauchy‖ attempted to prove the false theorem that the norm of the remainder obtained on dividing one complex number [8] by another can always be made less than the norm of the divisor. He drew the false conclusion that a product of complex integers [8] can be factored into complex primes in a single manner, and hence that all the laws of divisibility of ordinary integers hold for these complex integers. Next,¶ he assumed that the preceding results hold for a given n and developed at length the conclusions (often false), admitting at the end of the final paper that the basal theorem is false for $n = 23$.

5. **Difficulties presented by an example.** It will tend to concreteness to verify in a simple example the fact, so contrary to the intuitions of the able mathematicians just cited, that the laws of ordinary integers may fail for algebraic integers. As the first case of failure for the algebraic integers [8], determined by an nth root of unity, occurs for $n = 23$ and thus presents too much computation to serve as a simple illustration, we shall pass to the simpler example of the set S of all quadratic integers

* Comptes Rendus, Paris, 24, 1847, 899; Jour. de math., 12, 1847, 136.

† K. Hensel, Gedächtnisrede auf E. E. Kummer, Abh. Geschichte Math. Wiss., 29, 1910, p. 22.

‡ Comptes Rendus, Paris, 24, 1847, 430–4.

§ Ibid., 469–481; Oeuvres (1), 10, 240–254.

‖ Ibid., 516–528; Oeuvres (1), 10, 254–268.

¶ Ibid., 578–84, 633–6, 661–6, 996–9, 1022–30; Oeuvres (1), 10, 268–285, 296–308.

$a + b\theta$, where $\theta = \sqrt{-5}$ and a, b are ordinary integers. We have two distinct ways of factoring 9 into indecomposable numbers of the set S, viz.,

[9] $$9 = 3 \cdot 3 = (2 + \theta)(2 - \theta).$$

By an indecomposable number N of the set S we mean one having no factor in S other than N, $-N$, $+1$, -1. Suppose that

$$2 + \theta = (x + y\theta)(z + w\theta),$$

where x, y, z, w are ordinary integers. Then

$$2 - \theta = (x - y\theta)(z - w\theta)$$

and, by multiplication,

[10] $$9 = (x^2 + 5y^2)(z^2 + 5w^2).$$

But $x^2 + 5y^2 = 3$ is evidently not solvable in ordinary integers. Hence one of the factors of the right member of [10] is unity and the other is 9, so that one of the assumed factors of $2 + \theta$ is ± 1. In the same manner, the assumption that 3 is decomposable leads to equation [10], so that one of the two factors is ± 1. Hence the number 9 has the two distinct sets [9] of indecomposable factors in S.

Although 3 is indecomposable, it does not have the true character of a quadratic prime, since it divides the final product [9] without dividing either factor $2 \pm \theta$.

Again, there exists no number δ of S which plays the rôle of a greatest common divisor of 9 and $t = 3 - 6\theta$, so that 9 and t are divisible by δ, while every common divisor of 9 and t is a divisor of δ. In fact, the only factors in S of 9 are 1, 3, 9, $2 \pm \theta$ and their negatives; the only factors of t are 1, 3, $1 - 2\theta$, $2 - \theta$, $4 - \theta$, t and their negatives; so that the only common factors are ± 1, ± 3, $\pm (2 - \theta)$, no one of which is divisible by the remaining five (as shown above).

Hence the laws of arithmetic fail in several respects for the set S.

6. **Difficulties removed by use of Kummer's ideal numbers.** It was the fundamental discovery of Kummer* that the set of all complex integers defined by an nth root of unity could be so enlarged by the introduction of ideal numbers that unique factorization into primes would prevail in the enlarged set, which would therefore obey the laws of arithmetic as regards multiplication and division. Kummer had in mind immediate applications to Fermat's theorem and the higher reciprocity law.

While Kummer introduced ideal numbers only in the case of complex

* Berichte Ak. Wiss. Berlin, 1845; reprinted in Jour. für Math., 35, 1847, 319, 327. Jour. de math., 12, 1847, 185–212.

numbers defined by a root of unity, his method is applicable to the simpler example of § 5, as shown in detail by Dedekind.*

The difficulties encountered in § 5 can be overcome by the introduction of ideal prime numbers α, β, γ, such that

$$[11] \qquad 3 = \alpha\beta, \qquad 2 + \theta = \alpha^2, \qquad 2 - \theta = \beta^2, \qquad 1 - 2\theta = \beta\gamma.$$

Now each member of [9] decomposes further into $\alpha^2\beta^2$, so that there is now only one decomposition of 9 into ideal primes. Moreover, 9 and $3 - 6\theta = \alpha\beta^2\gamma$ now have the greatest common ideal divisor $\alpha\beta^2$.

Kummer did not define the ideal α itself, but gave a general method which when applied to our example affords a definite rule to decide whether or not a quadratic integer $\omega = x + y\theta$ is divisible by α, the test for divisibility being that $(1 + \theta)\omega \equiv 0 \pmod 3$, viz., $x + y \equiv 0 \pmod 3$. Similarly, ω is said to have the ideal factor β if and only if $(1 - \theta)\omega \equiv 0$, viz., $x - y \equiv 0 \pmod 3$. Thus ω has both factors α and β if and only if $x \equiv y \equiv 0 \pmod 3$, i. e., if ω is divisible by 3, and this accords with our agreement that $\alpha\beta = 3$. In like manner, ω is said to be divisible by α^n if and only if $(1 + \theta)^n\omega \equiv 0 \pmod{3^n}$; in particular, ω is divisible by α^2 if and only if

$$(1 + \theta)^2\omega = -4x - 10y + (2x - 4y)\theta \equiv 0 \pmod 9,$$

viz., if and only if $x \equiv 2y \pmod 9$. But the latter is seen to be a necessary and sufficient condition that ω be divisible by $2 + \theta$ (the quotient being a quadratic integer). Hence in testing for divisors we may identify α^2 with $2 + \theta$; and similarly β^2 with $2 - \theta$, since either is a factor of ω if and only if $x \equiv -2y \pmod 9$. Finally, our tests show at once that $1 - 2\theta$ is divisible by β, but not by β^2 or α.

Having now justified all the formulas [11], we have explained and removed the particular difficulties met in § 5. But the factorization of new numbers of our set S requires the definition of new ideal numbers. An exhaustive investigation would be quite lengthy; moreover, Dedekind has emphasized the delicacy of the subject and the constant need of the greatest circumspection. What precedes may suffice to indicate the point of view of Kummer. It has been completely superceded by the standpoint of Dedekind, which is more concrete, simpler and more general. Not that the fundamental results of Kummer have lost one whit of their importance; a reader of his papers has only to give to his terms the modern interpretation.

7. **Dedekind's ideals.** With Dedekind, an ideal is defined explicitly in terms of the given numbers and hence is more concrete and tangible than the ideal numbers of Kummer, which were not defined themselves

* Bull. sc. math. astr., 11, 1876, 278; (2), 1, I, 1877, 17, 69, 144, 207.

but their possible occurrence as factors determined. Moreover, Dedekind's method applies to all algebraic domains and not merely to Kummer's case of domains defined by roots of unity. Accordingly we can select as a medium for our introduction a very simple domain, which shall present the typical difficulties.

We shall again consider the set S of all quadratic integers $a + b\theta$, where $\theta = \sqrt{-5}$, and a, b are (ordinary) integers. Just as the number 3 determines uniquely all its multiples $3x + 3y\theta$ in S, where x and y range over all integers, so any number μ of S corresponds uniquely to the totality of its multiples in S, a totality σ called the principal ideal (μ) and evidently having the following two properties:

A. The sum and difference of any two (equal or distinct) numbers of the set σ are themselves numbers of the set σ.

B. Every product of a number of the set σ by a number of the entire set S is a number of the set σ.

In other words, the set σ is closed under addition and subtraction, as well as under multiplication by numbers of S. Any set of numbers of S will be called an ideal if it has these two properties and is not composed exclusively of the number zero.

The principal ideals (μ) correspond to the numbers μ of S. It will turn out that there exist further ideals and they play the rôle of Kummer's intangible ideal numbers. The principal and other ideals together furnish an enlarged system of elements obeying all the laws of arithmetic relating to divisibility.

8. **Explicit determination of all the ideals.** Since the product of any quadratic integer by its conjugate is an (ordinary) integer, it follows from property B that any ideal σ contains integers. Let k be the greatest common divisor of all the integers in σ, so that k is a linear function of these integers. Then, by property A, k occurs in σ. Likewise, if m is the greatest common divisor of the coefficients of θ in the various quadratic integers in σ, then σ contains $l + m\theta$, where l is some integer. Thus, by property A, σ contains the totality $[k, l + m\theta]$ of the linear homogeneous functions of k and $l + m\theta$ with integral coefficients. Moreover, σ coincides with that totality. For, let $a + b\theta$ be any number of σ. If $b = 0$, a is a multiple of k. If $b \neq 0$, then $b = qm$, so that σ contains

$$a + b\theta - q(l + m\theta) = a - ql,$$

which, being an integer in σ, is a multiple of k.

It remains to require that $\sigma = [k, l + m\theta]$ shall have also property B. By the bracket notation, the products of the numbers of σ by an integer are in σ. Hence we may restrict the proof to products of numbers in

σ by θ, and thus require that $k\theta$ and $(l + m\theta)\theta = -5m + l\theta$ shall be in σ. The coefficients k and l must be multiples of m. Let $k = ma$, $l = bm$. Then $k\theta = a(l + m\theta) - bk$ is in σ, while

$$-5m + l\theta = b(l + m\theta) - m(b^2 + 5)$$

is in σ if and only if $m(b^2 + 5)$ is divisible by k. Hence

$$[12] \qquad \sigma = [ma, m(b + \theta)], \qquad b^2 \equiv -5 \pmod{a},$$

is the desired explicit formula for any ideal. Evidently we may suppress multiples of a from b at will. If $a = 1$, we may therefore set $b = 0$ and obtain $[m, m\theta]$, which is another notation for the principal ideal (m).

9. **Multiplication of ideals.** Recalling that the principal ideal (μ) is to take the place of the number μ of S, we shall evidently desire that multiplication of ideals shall be such that it will give in particular $(\mu)(\lambda) = (\mu\lambda)$. Accordingly we define multiplication of ideals in general as follows: If ρ ranges over the numbers of an ideal σ, and ρ' over the numbers of an ideal σ', then the products $\rho\rho'$ and their sums and differences form an ideal called the product of σ and σ', and designated $\sigma\sigma'$.

In particular, the product of [12] by the conjugate ideal

$$\sigma_1 = [ma, m(b - \theta)]$$

is the aggregate of the linear functions with integral coefficients of

$$m^2a^2, \qquad m^2a(b - \theta), \qquad m^2a(b + \theta), \qquad m^2(b^2 + 5).$$

Write c for the integer $(b^2 + 5)/a$. Then

$$\sigma\sigma_1 = [m^2a^2, 2m^2ab, m^2ac, m^2a(b + \theta)].$$

The greatest common divisor of the first three integers is m^2ag, if g denotes that of a, $2b$, c. Since $b^2 + 5 = ac$, g^2 divides 20, and $g = 1$ or 2. But if a, c were both even, $b^2 + 5 \equiv 0 \pmod 4$, whereas $b^2 \equiv 0$ or $1 \pmod 4$. Hence $g = 1$. The greatest common divisor of three numbers equals a linear combination of them. Thus

$$\sigma\sigma_1 = [m^2a, m^2a(b + \theta)] = [m^2a, m^2a\theta] = (m^2a).$$

Hence *the product of any ideal and its conjugate is a principal ideal.*

10. **Division of ideals.** Every number of the product $\rho\sigma$ of two ideals belongs to the ideal ρ, as follows at once from the definition of multiplication of ideals and properties B and A. Conversely, *if every number of an ideal τ belongs to an ideal ρ, there exists an ideal σ such that $\rho\sigma = \tau$,* and τ is said to be divisible by ρ. For, if ρ_1 is the conjugate to ρ, the numbers of $\tau\rho_1$ belong to the principal ideal $\rho\rho_1 = (r)$, so that the numbers

of $\tau\rho_1$ are $s_1 r$, $s_2 r$, $\cdots$, where the s's are quadratic integers. Since properties A and B hold for the ideal $\tau\rho_1$, we have

$$s_1 r + s_2 r = s_i r, \qquad s_1 r - s_2 r = s_j r, \qquad s(s_1 r) = s_k r,$$

for any quadratic integer s, where s_i, s_j, s_k belong to the set s_1, s_2, $\cdots$. Cancelling the factor r, we see that the set of numbers s_1, s_2, $\cdots$ has the characteristic properties A, B of an ideal σ. Hence $\tau\rho_1 = \sigma(r) = \sigma\rho\rho_1$, whence $\tau = \sigma\rho$. For, an equation $\alpha\beta = \alpha\gamma$ in ideals implies that $\beta = \gamma$. To show this, let α_1 be the ideal conjugate to α, so that $\alpha\alpha_1$ is a principal ideal (a). Then $\alpha_1\alpha\beta = \alpha_1\alpha\gamma$ or $(a)\beta = (a)\gamma$, and the products of the numbers of β by a are identical with the products of the numbers of γ by a, whence $\beta = \gamma$.

An ideal τ is divisible by only a finite number of ideals ρ. For, if τ_1 is the ideal conjugate to τ, $\tau\tau_1$ is a principal ideal (t), where t is an integer. If $\tau = \rho\sigma$, then $(t) = \rho \cdot \sigma\tau_1$, and, by the first remark in this section, t belongs to the ideal ρ. But t belongs only to a finite number of ideals $[k, l + m\theta]$, since (§ 8) k is an integer dividing t, and m is an integer dividing k, while l can be restricted to the values $0, 1, \cdots, k - 1$.

11. **Unique factorization of an ideal into primes.** An ideal, different from the principal ideal (1) and divisible by no ideal other than itself and (1), is called a prime ideal.

If the prime ideal π divides a product $\rho\sigma$, it divides ρ or σ. Suppose that π does not divide ρ. Then the ideal composed of the numbers of both π and ρ and their sums and differences contains all the numbers of π and hence (§ 10) is a divisor of π; being distinct from π, it is (1). Hence $1 = p + r$, where p is some number of π, and r some number of ρ. Let s be any number of σ. Then $s = ps + rs$. By hypothesis, rs occurs in π. By property B, ps occurs in π. Hence by property A, s occurs in π. Hence (§ 10), σ is divisible by π.

An ideal not a prime and different from (1) is said to be composite. *Every composite ideal σ can be expressed in one and but one way as a product of a finite number of prime ideals.* Since σ has a divisor σ_1, distinct from (1) and σ, we have $\sigma = \sigma_1\sigma_2$, where σ_2 is distinct from (1). If one of the ideals σ_1, σ_2 is not a prime, it equals a product of two ideals, and we get $\sigma = \sigma_1'\sigma_2'\sigma_3'$. If one of the σ_i' is not a prime, it equals a product of two ideals; etc. This process must terminate. For, by the final result of § 10, σ is divisible by only a finite number n of ideals, whereas a relation $\sigma = \tau_1\tau_2 \cdots \tau_{n+1}$, in which each ideal τ_i is distinct from (1), would require that σ have the $n + 1$ distinct factors τ_1, $\tau_1\tau_2$, $\cdots$, $\tau_1 \cdots \tau_{n+1}$. Hence our process must lead to a prime ideal factor of σ. Applying the same result to the quotient, etc., we see that σ is a product of a finite

number of prime ideals. There cannot be a second such factorization of σ into prime ideals in view of the first theorem of this section.

12. **Prime ideals.** Let p be the least positive integer contained in the prime ideal π. Then p is a prime. For, if $p = rs$, where r and s are integers > 1, π divides (p) by § 10 and hence also (r) or (s), and π would contain the positive integer $r < p$ or $s < p$. Let π be given by formula [12]. Then $ma = p$, so that either $m = p$, $a = 1$, or $m = 1$, $a = p$. In the first case, $\pi = [p, p(b + \theta)]$ is the principal ideal (p). In the second case, $\pi = [p, b + \theta]$, where $b^2 \equiv -5 \pmod{p}$, and, if π' is the conjugate of π, $\pi\pi' = (p)$ by § 9. Conversely, if $(p) = \pi\pi'$, π is a prime ideal. For, if $\pi = \rho\sigma$, and $\rho\rho' = (r)$, $\sigma\sigma' = (s)$, then $p = rs$ would be composite. Hence *if p is a prime $\neq 2, 5$, (p) is the product of two distinct conjugate prime ideals or is itself a prime ideal according as -5 is a quadratic residue or non-residue of p; while* (2) *and* (5) *are the squares of the prime ideals* $[2, 1 + \theta]$ *and* $[5, \theta]$ *respectively. All prime ideals are obtained in this way from the primes p.*

13. **Explanation of the difficulties in § 5.** We pass from the quadratic integers 3, $2 \pm \theta$ to the corresponding principal ideals (3), $(2 \pm \theta)$. By § 12, $(3) = \alpha\beta$, where $\alpha = [3, -1 + \theta]$, $\beta = [3, 1 + \theta]$. Since $(\mu) = [\mu, \mu\theta]$,

$$(2 + \theta) = [2 + \theta, -5 + 2\theta] = [9, 2 + \theta] = \alpha^2 = [9, -3 + 3\theta, -4 - 2\theta].$$

Changing the sign of θ, we see that $(2 - \theta) = \beta^2$. Next,

$$(1 - 2\theta) = [1 - 2\theta, 10 + \theta] = [21, 10 + \theta] = \beta\gamma,$$

where $\gamma = [7, 3 + \theta]$ is one of the prime ideal factors of (7), by § 12. Hence the ideal (9) has the single factorization $\alpha^2\beta^2$ into prime ideals, while (9) and $(3 - 6\theta) = \alpha\beta^2\gamma$ have the greatest common ideal divisor $\alpha\beta^2$. The present explanation of the former difficulties is thus notationally the same as in § 6, but we have now used concrete prime ideals α, β, γ in place of Kummer's intangible ideal numbers.

14. **Classes of ideals.** Two ideals ρ and σ are called equivalent if there exist principal ideals (r) and (s) such that $\rho(r) = \sigma(s)$. Any two principal ideals are therefore equivalent. If also ρ is equivalent to τ, with $\rho(q) = \tau(t)$, then σ is equivalent to τ since $\sigma(sq) = \rho(rq) = \tau(rt)$. Hence all ideals equivalent to a given one are equivalent to each other and are said to form a class of ideals. The principal class contains all the principal ideals and no others. For, if σ is equivalent to (1), $\sigma(s) = (r)$, so that the number r of the product $\sigma(s)$ is in (s), whence r is divisible by s, and $\sigma = (r/s)$.

Without resorting to any device, we shall give a direct determination

of the classes of ideals for the domain defined by $\theta = \sqrt{-5}$. If (α) is any principal ideal, we may set $\alpha = m(A + B\theta)$, where A and B are relatively prime integers. We can choose integers r, s such that

$$\begin{vmatrix} s & -r \\ -A & B \end{vmatrix} = sB - rA = 1.$$

Hence

$$(\alpha) = [\alpha, \alpha\theta] = [s\alpha - r\alpha\theta, -A\alpha + B\alpha\theta] = [m(b + \theta), -ma],$$

$$a = A^2 + 5B^2, \qquad b = sA + 5rB.$$

Thus the principal ideals are given* by [12] in which $a = A^2 + 5B^2$, where A and B are relatively prime. Since 2 is not a value of a, the ideal $\rho = [2, 1 + \theta]$ is not a principal ideal. We next find all the ideals β equivalent to ρ, i. e., for which $\beta(\gamma) = \rho(\delta)$. Let (γ_1) be the ideal conjugate to (γ), so that $(\gamma)(\gamma_1) = (k)$, where k is an integer. Then $\beta(k) = \rho(\alpha)$, where $\alpha = \delta\gamma_1$. Hence we must examine the product

$$\begin{aligned}\rho(\alpha) &= [2, 1 + \theta][ma, m(b + \theta)] \\ &= [2ma, 2m(b + \theta), ma(1 + \theta), m(b - 5) + m(1 + b)\theta].\end{aligned}$$

First, let a be odd, $a = 2c + 1$. Since we may add the modulus a to b, we may assume that the root b is odd. Since

$$a(1 + \theta) = c(2b + 2\theta) + b + \theta + 2a(1 - b)/2,$$

$$b - 5 + (1 + b)\theta = (1 + b)(b + \theta) - (b^2 + 5),$$

and $b^2 + 5$ is an even multiple of a, we have

[13] $$\rho(\alpha) = [2ma, m(b + \theta)], \qquad b^2 \equiv -5 \pmod{2a}.$$

Second, let a be even, $a = 2c$. Since a divides $b^2 + 5$, b is odd, and $b^2 + 5 \equiv 2 \pmod 4$, so that $(b^2 + 5)/a$ is odd. Since

$$a(1 + \theta) = c(2b + 2\theta) + 2a(1 - b)/2,$$

$$b - 5 + (1 + b)\theta = \tfrac{1}{2}(b + 1)(2b + 2\theta) - (b^2 + 5),$$

we have

[14] $$\rho(\alpha) = [2m \cdot a/2, 2m(b + \theta)], \qquad b^2 \equiv -5 \pmod{a/2}.$$

Thus the ideals β equivalent to ρ are those for which $\beta(k)$ is of the form [13] or [14], where k is an integer dividing m or $2m$ respectively. But m ranges over all integers. Hence the ideals equivalent to ρ are given by [13] and [14], with m and $2m$ replaced by an arbitrary integer M, while a is any integer of the form $A^2 + 5B^2$, with A and B relatively

* As a check, note that $b^2 + 5 = b^2 + 5(sB - rA)^2 = a(s^2 + 5r^2)$.

prime. For a odd, $1 \equiv A - B \pmod 2$ and

$$2a = 2x^2 + 2xy + 3y^2, \qquad x = A - B, \qquad y = 2B,$$

so that x and y are relatively prime. For a even, $A \equiv B \equiv 1 \pmod 2$ and

$$\frac{a}{2} = 2x^2 + 2xy + 3y^2, \qquad x = \frac{A - B}{2}, \qquad y = B,$$

so that x and y are relatively prime integers. Combining the two cases, we conclude that all the ideals equivalent to $\rho = [2, 1 + \theta]$ are

$$[15] \quad [MN, M(b + \theta)], \qquad b^2 \equiv -5 \pmod N, \qquad N = 2x^2 + 2xy + 3y^2,$$

where x, y are relatively prime integers.

The class C of the principal ideals and the class C' of the ideals [15] together give all the ideals [12]. For, if a has any value admissible in [12], not merely the preceding special value, there exists an integer l such that $b^2 = -5 + al$ and the form $ax^2 + 2bxy + ly^2$ is of determinant -5 and hence* can be transformed into $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ by a linear transformation with integral coefficients of determinant unity. Our general form reduces to a for $x = 1$, $y = 0$. Hence a can be represented by one of our two special forms by means of relatively prime integers x, y. If it be the first form, the ideal [12] has been shown to be a principal ideal; if it be the second form, the ideal is of type [15] and is equivalent to $[2, 1 + \theta]$.

All the ideals have been distributed into two classes C and C' and an explicit formula has been given for the ideals in each class. The two classes can be distinguished very simply as follows. For an ideal [12] in C, $a \equiv x^2 \pmod 5$, so that a is a quadratic residue of 5. For an ideal [15],

$$2N = (2x + y)^2 + 5y^2,$$

so that $2N$ is a residue and N is a non-residue of 5 if N be prime to 5.

The above method of proving that there are only two classes of ideals in the domain employed has not only the advantage of being elementary and exhibiting explicitly all the ideals in each class, but also of illustrating the essential† identity of the problems to find the number of classes of ideals in a quadratic domain of discriminant d and the number of classes of binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = d$.

* The two forms are the only reduced forms, i. e., having $l \geqq a \geqq 2|b|$.

† In the present case, every number has a positive norm. But in general, we must employ narrowly equivalent ideals (Dirichlet-Dedekind, Zahlentheorie, p. 578, p. 584) whose ratio is a number of positive norm. To every narrow class of ideals in a quadratic field of discriminant d corresponds one and but one class of quadratic forms of discriminant d capable of representing positive numbers.

15. **Another method for the preceding problem.** The usual method of finding the number of classes of ideals in our domain $F(\sqrt{-5})$ of discriminant $-5\cdot 4$ is based upon the fact that every ideal [12] contains a number $\alpha = r + s\theta \neq 0$ whose norm $r^2 + 5s^2$ does not exceed $m^2a\sqrt{20}$. We may take

$$\alpha = xma + ym(b + \theta), \qquad r = m(ax + by), \qquad s = my.$$

By the well-known theorem due to Minkowski,* we can choose rational integers x, y not both zero such that

$$|\, ax + by \,| \leqq \sqrt{a\sqrt{5}}, \qquad |\, y \,| \leqq \sqrt{a/\sqrt{5}},$$

since the determinant a of the linear functions equals the product of the two radicals. Hence, as desired,

$$(ax + by)^2 + 5y^2 \leqq a\sqrt{20}.$$

Consider an ideal A of any class K of ideals. Call B the ideal [12] which is conjugate to A, so that BA is a principal ideal (q), by § 9. As just proved, B contains a number α of norm $\leqq m^2a\sqrt{20}$. Then (§ 10), (α) is divisible by B; let Q be the quotient. The norm of [12] is m^2a by definition. It is easily verified that the product of the norms of B and Q equals the norm of their product (α). Thus [norm Q] $\leqq \sqrt{20}$. From $BQ = (\alpha)$, $BA = (q)$ follows $A(\alpha) = Q(q)$, so that A and Q are equivalent ideals. Hence any class K contains an ideal of norm $\leqq \sqrt{20}$, and hence an ideal [12] whose norm m^2a equals 1, 2, 3 or 4. If $a = 1$, the ideal is a principal ideal (§ 10). If $a > 1$, $m = 1$, while $a = 4$ is excluded since $b^2 \equiv -5 \pmod 4$ is not solvable. If $a = 2$, we have $b = 1$ and the ideal is $[2, 1 + \theta] = \rho$. If $a = 3$, we have $b = \pm 1$ and the ideals are $[3, 1 + \theta] = \beta$ and $[3, -1 + \theta] = \beta'$. Then $\beta\beta' = (3)$ and

$$\rho\beta' = [6, -2 + 2\theta, 3 + 3\theta] = [6, \theta - 1] = (\theta - 1).$$

Multiply this by β. Hence $\rho(3) = \beta(\theta - 1)$, so that ρ and β are equivalent. Changing the sign of θ throughout, we see that ρ and β' are equivalent. Hence the principal class and the class containing ρ are the only classes.

16. **Kummer's class number H.** For the domain defined by an imaginary λth root α of unity, where λ is an odd prime, Kummer† proved that

* Cf. Hurwitz, Göttingen Nachrichten, 1897; J. Sommer, Vorlesungen über Zahlentheorie, 1907, p. 71.

† Bericht Akad. Wiss. Berlin, 1847, 305–319. Jour. für Math., 40, 1850, 93–129. Jour. de math., 16, 1851, 454–498.

the number of classes of ideals is the product $H = h_1 h_2$ of the two integers

$$h_1 = \frac{P}{(2\lambda)^{\mu-1}}, \qquad h_2 = \frac{D}{\Delta},$$

where $\mu = (\lambda - 1)/2$, and P, D, Δ are defined as follows. Let β be a primitive root of $\beta^{\lambda-1} = 1$ and g a primitive root of λ. Then

$$P = \prod_{j=1}^{\mu} \phi(\beta^{2j-1}), \qquad \phi(\beta) = 1 + g_1\beta + g_2\beta^2 + \cdots + g_{\lambda-2}\beta^{\lambda-2},$$

where g_i is the least positive residue of g^i modulo λ. Next,

$$e(\alpha) = \sqrt{\frac{(1 - \alpha^g)(1 - \alpha^{-g})}{(1 - \alpha)(1 - \alpha^{-1})}}$$

is a complex unit (a divisor of 1). Then, if lx denotes $\log x$,

$$D = \begin{vmatrix} le(\alpha) & le(\alpha^g) & \cdots & le(\alpha^{g^{\mu-2}}) \\ le(\alpha^g) & le(\alpha^{g^2}) & \cdots & le(\alpha^{g^{\mu-1}}) \\ \cdot & \cdot & \cdots & \cdot \\ le(\alpha^{g^{\mu-2}}) & le(\alpha^{g^{\mu-1}}) & \cdots & le(\alpha^{g^{2\mu-4}}) \end{vmatrix}.$$

Let $\epsilon_1(\alpha), \cdots, \epsilon_{\mu-1}(\alpha)$ be units such that products of powers of them multiplied by $\pm \alpha^m$ give all the units. Then

$$\Delta = \begin{vmatrix} l\epsilon_1(\alpha) & \cdots & l\epsilon_{\mu-1}(\alpha) \\ \cdot & \cdots & \cdot \\ l\epsilon_1(\alpha^{g^{\mu-2}}) & \cdots & l\epsilon_{\mu-1}(\alpha^{g^{\mu-2}}) \end{vmatrix}.$$

It is shown that h_1 is divisible by λ if and only if λ divides the numerator of one of the first $(\lambda - 3)/2$ Bernoullian numbers $B_1 = 1/6$, $B_2 = 1/30$, $\cdots$; while if h_2 is divisible by λ also h_1 is, but not conversely.

PART III.

Application of Algebraic Numbers to Fermat's Last Theorem.

17. Kummer* proved that $x^\lambda + y^\lambda = z^\lambda$ is impossible in integers if λ is an odd prime not dividing H (§ 16) and hence not the numerator of any one of the first $(\lambda - 3)/2$ Bernoullian numbers. To indicate the nature of the proof for the case in which x, y, z are prime to λ, denote the factor $z - \alpha^j y$ of $z^\lambda - y^\lambda$ by f_j. The greatest common ideal divisor G

* Bericht Akad. Wiss. Berlin, 1847, 132–9. The proof has been given in modern form, by use of Dedekind's ideals, by D. Hilbert, Jahresbericht Deutschen Math.-Vereinigung, 4, 1894–5, 517–25. Cf. E. Schönbaum, Casopis, 37, 1908, 384–506 (Bohemian).

of any two (f_j) is that of (z) and (y). The product of the (f_j) is $(x)^\lambda$. Hence $(f_j) = GJ_j^\lambda$, where no two J's have a common factor. Thus $J_j{}^\lambda$ and $J^\lambda{}_{\lambda-1}$ are equivalent ideals. But the Hth power of any ideal is a principal ideal, so that J_j^H and $J^H{}_{\lambda-1}$ are equivalent. Since λ does not divide H, it follows that J_j and $J_{\lambda-1}$ are equivalent. Thus (f_j) and $(f_{\lambda-1})$ are proportional to the λth powers of two principal ideals. It follows readily that

$$f_j = \alpha^{e_j} u_j \tau_j{}^\lambda \qquad (j = 0, 1, \cdots, \lambda - 2),$$

where u_j is a real unit and τ_j a number of our domain $F(\alpha)$. A discussion of these equations between ordinary complex numbers leads to a contradiction.

Cauchy* stated that $a^n + b^n + c^n = 0$ is impossible in relatively prime integers not divisible by the odd prime n if

$$1 + 2^{n-4} + 3^{n-4} + \cdots + \left(\frac{n-1}{2}\right)^{n-4}$$

is not divisible by n [i. e., if B_k is not divisible by n for $k = (n-3)/2$].

Kummer† proved that Fermat's equation for an odd prime exponent not dividing H has no solution in complex integers $a_0 + a_1\alpha + a_2\alpha^2 + \cdots$, where $\alpha^\lambda = 1$. Thus there is no solution for $\lambda < 100$, except perhaps for $\lambda = 37, 59, 67$.

The French Academy of Sciences‡ had offered a gold medal of value 3000 francs for a complete proof of Fermat's last theorem. The prize was awarded to Kummer in 1857 for his investigations on complex integers, although he had not been a competitor.

Kummer§ proved that for any relatively prime integral solutions of $x^\lambda + y^\lambda = z^\lambda$, where λ is an odd prime,

$$[16] \qquad B_{(\lambda-i)/2} P_i(x, y) \equiv 0 \pmod{\lambda} \qquad (i = 3, 5, \cdots, \lambda - 2),$$

where B_j is the jth Bernoullian number and $P_i(x, y)$ is the homogeneous polynomial of degree i for which

$$\left(\frac{d^i \log (x + e^v y)}{dv^i}\right)_{v=0} = \frac{P_i(x, y)}{(x + y)^i}.$$

He proved that Fermat's equation is impossible in integers for odd prime exponents λ which satisfy the following three conditions. (i) The factor h_1 of the class number H is divisible by λ, but not by λ^2. (ii) For

* Comptes Rendus, Paris, 25, 1847, 181; Oeuvres (1), 10, 364. Genocchi, Jour. für Math., 99, 1886, 316.

† Jour. für Math., 40, 1850, 130–8; Jour. de Math., 16, 1851, 488–98.

‡ Comptes Rendus, 29, 1849, 23; 30, 1850, 263–4; 44, 1857, 158.

§ Abhand. Ak. Wiss. Berlin, 1857, Math., 41–74.

$e(\alpha)$, g and μ defined in § 16, and for the integer $\nu < (\lambda - 1)/2$ such that $B_\nu \equiv 0 \pmod{\lambda}$, there exists an ideal with respect to which as a modulus the unit

$$E_\nu(\alpha) = \prod_{k=0}^{\mu-1} e(\alpha^{g^k}) g^{-2k\nu}$$

is not congruent to a λth power, whence the second factor h_2 of H is not divisible by λ. (iii) The Bernoullian number $B_{\nu\lambda}$ is not divisible by λ^3. All three conditions are satisfied when $\lambda = 37, 59, 67$, the values < 100 of λ for which he had not previously proved Fermat's theorem.

D. Mirimanoff* proved Fermat's theorem for the exponent 37 by use of ideals.

E. Maillet† proved that Fermat's equation with the exponent λ^t is impossible in complex integers, prime to λ, formed from a λth root of unity, if λ is a prime > 3 and λ^{t-1} is the highest power of λ dividing the class number H.

Maillet‡ found by Kummer's method a variety of general values of c for which $x^\lambda + y^\lambda = cz^\lambda$ is impossible when λ is a regular prime (i. e., not a divisor of H); also§ when c equals λ or specified multiples of λ, for various λ's.

Mirimanoff‖ considered

$$x^\lambda + y^\lambda + z^\lambda = 0 \tag{17}$$

for the case in which no one of the integral solutions x, y, z is divisible by the odd prime λ. By use of Kummer's congruences [16], he proved that [17] is impossible in integers prime to λ if at least one of the Bernoullian numbers¶ $B_{\nu-1}, B_{\nu-2}, B_{\nu-3}, B_{\nu-4}$ is not divisible by λ, where

$$\nu = (\lambda - 1)/2;$$

also, for every $\lambda < 257$. In terms of Kummer's $P_i(t) = P_i(1, t)$, he defined the polynomials

$$\phi_i(t) = (1 + t)^{\lambda-i} P_i(t) \equiv \sum_{k=1}^{\lambda-1} (-1)^{k-1} k^{i-1} t^k \quad (i = 2, 3, \cdots, \lambda - 1) \tag{18}$$

modulo λ. Thus Kummer's criterion [16] is equivalent to the following. If [17] has solutions prime to λ, each of the six ratios $t = x/y, \cdots, z/x$

* Jour. für Math., 111, 1893, 26–30.

† Assoc. franc. avanc. sc., 26, 1897, II, 156–168.

‡ Acta Mathematica, 24, 1901, 247–256.

§ Annali di mat. (3), 12, 1905, 145–178.

‖ Jour. für Math., 128, 1905, 45–68.

¶ If $B_{\nu-1}$ or $B_{\nu-2}$ is not divisible by λ, the conclusion was drawn by Kummer in his 1857 paper.

satisfies the congruences

$$[19] \qquad B_{(\lambda-i)/2}\,\phi_i(t) \equiv 0 \pmod{\lambda} \qquad (i = 3, 5, \cdots, \lambda - 2).$$

An equivalent criterion not involving Bernoullian numbers is that each of the six ratios satisfies the congruences

$$[20] \quad \phi_{\lambda-1}(t) \equiv 0, \qquad \phi_{\lambda-i}(t)\phi_i(t) \equiv 0 \pmod{\lambda} \qquad (i = 2, 3, \cdots, \nu).$$

A. Wieferich* proved by means of [19] that, if Fermat's equation has solutions each prime to the exponent p, then

$$[21] \qquad 2^{p-1} \equiv 1 \pmod{p^2}.$$

The kth derivative with respect to v of

$$te^v - t^p e^{pv} = (1 + te^v)\sum_{i=1}^{p-1}(-1)^{i-1}t^i e^{iv}$$

gives for $v = 0$, on writing θ for $(1 + t)/t$,

$$\theta\phi_{k+1} + \binom{k}{1}\phi_k + \binom{k}{2}\phi_{k-1} + \cdots + \binom{k}{k}\phi_1 = 1 - t^{p-1}p^k.$$

Taking $k = 0, 1, \cdots$ and solving these linear equations, we get

$$\phi_{k+1} \equiv \frac{(-1)^{k-1}k!\,F_k}{\theta^k} \pmod{p}, \qquad F_i = \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{i-1} & \alpha_i \\ \theta & \alpha_1 & \cdots & \alpha_{i-2} & \alpha_{i-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & \theta & \alpha_1 \end{vmatrix},$$

where $\alpha_i = 1/i!$. Let G_i be the determinant derived from F_i by replacing α_j in the rth row by $\binom{k-r+1}{j}$ for $r = 1, \cdots, i$. Thus $(k - i)!\,G_i = k!\,F_i$. By evaluating G_k, we find that

$$-\theta\phi_{k+1} \equiv -H_{k+1} + \theta\lambda^k + \binom{k}{1}H_k\phi_2 + \cdots + \binom{k}{k-1}H_2\phi_k \pmod{p},$$

where $H_{i+1} = (1 + \lambda)^i - (\theta - 1)\lambda^i$, λ being arbitrary. Summing for $\lambda = 0, -1, 2, -3, \cdots, p - 1, -p$ and setting $\mathfrak{B}_{2j} = \Sigma(-\lambda)^{2j-1}$ and replacing k by $2k - 1$, we get

$$[22] \qquad \begin{aligned} -\theta\phi_{2k} \equiv -2\mathfrak{B}_{2k} + (2 - \theta)\Big\{&\binom{2k-1}{2}\mathfrak{B}_{2k-2}\phi_3 + \cdots \\ &+ \binom{2k-1}{2k-2}\mathfrak{B}_2\phi_{2k-1}\Big\} \pmod{p}. \end{aligned}$$

If B_j is the jth Bernoullian number, it is known that

$$\mathfrak{B}_{2j} \equiv (-1)^{j-1}B_j(2^{2j} - 1)/j \pmod{p}.$$

* Jour. für Math., 136, 1909, 293-302.

Hence, taking $k = (p-1)/2$ and applying [19], we get

$$2\mathfrak{B}_{p-1} \equiv \theta\phi_{p-1} \equiv \frac{\theta}{p}\{(1+t)^p - 1 - t^p\} \equiv 0 \pmod{p},$$

since t is the ratio of two values satisfying [17]. But $\mathfrak{B}_{p-1} \equiv (2^p-2)/p$.

D. Mirimanoff* employed Euler's expression for $1 - 2^{p-2} + 3^{p-2} - \cdots \pm y^{p-2}$ as a polynomial in y, took $y = 1, 2, \cdots, p-1$, multiplied the resulting equations by $t, t^2, \cdots, t^{p-1}$, added, multiplied the sum by $t-1$, and obtained

$$[1^{p-2} - 2^{p-2} + \cdots - (p-1)^{p-2}]t^p - \tfrac{1}{2}(t+1)\phi_{p-1}$$
$$= (t-1)\sum_{j=1}^{\nu-1}(-1)^{j-1}\binom{p-2}{2j-1}\frac{2^{2j}-1}{2j}B_j\phi_{p-2j} + (-1)^{\nu-1}\frac{2^p-2}{p-1}B_\nu\frac{t^p-1}{t+1},$$

where $\nu = (p-1)/2$ and ϕ_i is given by [18]. The final term is a multiple of p for every t; dropping it, we get [22] for $k = (p-1)/2$. Or, we may apply [19] and [20_1] and conclude that

$$0 \equiv 1^{p-2} - 2^{p-2} + \cdots - (p-1)^{p-2} \equiv (2^p-2)/p \pmod{p}.$$

G. Frobenius† deduced [21] from [19] and [20_1] by showing that

$$\sum_{r,\,s=0}^{\lambda-1}(-1)^{r-s}(r-s)^{\lambda-2}t^s$$

is congruent modulo λ, for every $t \neq 0, \pm 1$, to both

$$c = \phi_{p-1}(1), \qquad \frac{1+t}{1-t}c,$$

whence $c \equiv 0 \pmod{\lambda}$, which gives [21].

E. Hecke‡ proved that [17] is impossible in integers x, y, z each not divisible by the odd prime exponent λ such that the factor h_1 of H is divisible by λ, but not by λ^2.

D. Mirimanoff§ proved that if there are solutions of

$$x^p + y^p + z^p = 0$$

prime to p, each of the six ratios $x/y, \cdots$ is a root t of

$$[23] \qquad \prod_{i=1}^{m-1}(t+\alpha_i)\sum_{i=1}^{m-1}\frac{R_i}{t+\alpha_i} \equiv 0 \pmod{p}, \qquad R_i = \frac{\phi_{p-1}(-\alpha_i)}{(1-\alpha_i)^{p-1}},$$

* L'enseignement math., 11, 1909, 455–9.

† Sitzungs. Ak. Wiss. Berlin, 1909, 1222–4; Jour. für Math., 137, 1910, p. 314–6.

‡ Göttingen Nachrichten, 1910, 420–4.

§ Comptes Rendus, Paris, 150, 1910, 204–6. See his paper of 1911.

where $\alpha_1, \cdots, \alpha_{m-1}$ are the roots $\neq 1$ of $z^m = 1$; also,

$$q(m) = \frac{m^{p-1} - 1}{p} \equiv \sum_{i=1}^{m-1} \frac{R_i}{1 - \alpha_i} \pmod{p}.$$

For $m = 2$ or 3, the degree of [23] is < 2, whereas at least two of the six ratios are incongruent; thus [23] is an identity. Taking $t = -1$, we get $q(m) \equiv 0$. In addition to Wieferich's criterion $q(2) \equiv 0$, we have $q(3) \equiv 0$.

G. Frobenius* proved the last two criteria and deduced [19] from [16] more simply than had Mirimanoff. With Lucas,† set $b^{2n} = (-1)^{n-1}B_n$, $b^{2n+1} = 0$, $b^1 = -\frac{1}{2}$, so that the Bernoullian numbers are given by $(b + 1)^n - b^n = 0$ if $n > 1$. Set

$$F(x, y) = \sum_{r=0}^{p-1} \binom{y}{r} (x - 1)^r,$$

$$F(x, y)x^m = \sum_r \binom{y + m}{r} (x - 1)^r + (x - 1)^p G(x, y),$$

$$mxG_m(x) = G(x, mb) - G(0, mb)\frac{x^m - 1}{x - 1},$$

$$mF(x) = F(x, mb) - \{F(0, mb) - mpq\}(x - 1)^{p-1}.$$

Then

$$F(x)(x^m - 1) + \sum_{n=1}^{p-1} \frac{1 - x^n}{n} = (x - 1)^p x G_m(x),$$

from which the results of the paper follow. The six ratios of the three solutions prime to p of Fermat's equation satisfy the congruence $G_m(x) \equiv 0 \pmod{p}$ of degree $m - 2$. Hence, if $m = 2$ or 3, G_m vanishes identically. But $G_m(1) \equiv (1 - m^{p-1})/p$.

F. Bernstein‡ proved Fermat's theorem under assumptions milder than those used by Kummer in 1857. For the case in which one of the numbers x, y, z is divisible by the prime exponent λ, it suffices to assume that the number of classes of ideals for the field $k(Z)$ of the λ^2th roots of unity is divisible by λ, but not by λ^2; or, to assume that $k(Z)$ contains no class belonging to the exponent λ^2, while the number of classes for $k(\alpha + \alpha^{-1})$, where $\alpha^\lambda = 1$, is prime to λ. For the case in which x, y, z are prime to λ, it suffices to assume (i) the factor h_2 of the number H of classes in $k(\alpha)$ is divisible by λ, and (ii) if λ^μ is the highest power of λ dividing h_2, then in the Teilklassenkörper of the λ^μth degree every ideal of $k(\alpha)$, whose λth power is a principal ideal in $k(\alpha)$, is itself a principal ideal.

* Sitzungs. Ak. Wiss. Berlin, 1910, 200–8.

† Earlier in Blissard, Quar. Jour. Math., 1861, 279.

‡ Göttingen Nachrichten, 1910, 482–8, 507–16.

Ph. Furtwängler* proved, in extension of Kummer's work, that if $\alpha^l + \beta^l + \gamma^l = 0$, where α, β, γ are numbers, prime to $L = (\zeta - 1)$, of the field $k(\zeta)$, $\zeta^l = 1$, and if $\alpha \equiv a$, $\beta \equiv b$, $\gamma \equiv c \pmod{L}$, where a, b, c are rational, and if $k(\zeta)$ contains no ideal belonging† to the exponent $2j + 1$ modulo L, then, if x, y are any two of a, b, c,

$$\left[\frac{d^{2j+1} \log (x + e^v y)}{dv^{2j+1}}\right]_{v=0} \equiv 0 \pmod{l}.$$

By Mirimanoff's paper of 1905, this congruence can not hold when $j = 1, 2, 3$ or 4. Hence if $k(\zeta)$ does not contain ideals belonging to each of the exponents 3, 5, 7, 11, Fermat's equation is impossible in numbers prime to l in $k(\zeta)$. The same conclusion holds if the class number H is at most divisible by l^3.

Mirimanoff‡ reproduced his paper of 1910 and used his formula [23] to obtain results concerning $q(5)$ and $q(7)$. He proved that $\phi_{p-1}(t)$ is divisible by p not only when t is one of the six ratios $\tau = x/y, \cdots$, but also for $t = -\tau$ and $t = -\tau^2$. Finally, he proved Sylvester's§ formula

$$q(m) \equiv \sum_{n=1}^{p-1} \frac{x_n}{p - n} \pmod{p}, \qquad x_n \equiv \frac{n}{p} \pmod{m}.$$

Ph. Furtwängler‖ proved by use of Eisenstein's law of reciprocity for residues of lth powers, where l is an odd prime, that every integral divisor r of x_i satisfies

[24] $$r^{l-1} \equiv 1 \pmod{l^2}$$

if x_1, x_2, x_3 are relatively prime solutions $\neq 0$ of ${x_1}^l + {x_2}^l + {x_3}^l = 0$ and x_i is prime to l. Since one of the x's is divisible by 2, we have the criterion [21] of Wieferich. Next, every factor r of $x_i \pm x_k$ satisfies [24] if $x_i + x_k$ and $x_i - x_k$ are prime to l. Since one of the x's is divisible by 3 unless all three are congruent modulo 3, it follows from the two theorems that, if the x's are all prime to l, [24] holds for $r = 3$, which is the criterion of Mirimanoff.

S. Bohnicek† proved that integral numbers of the domain of the 2^nth roots of unity do not satisfy Fermat's equation with the exponent 2^{n-1}, $n > 2$.

* Ibid., 554–562.

† An ideal Q, prime to $L = (\zeta - 1)$, is said to belong to the exponent n modulo L if Q^l is a principal ideal (κ) such that $\kappa \equiv r_1 \pmod{L^n}$, while there exists no unit η in the field $k(\zeta)$ such that $\eta\kappa \equiv r_2 \pmod{L^{n+1}}$, where r_1 and r_2 are rational numbers.

‡ Jour. für Math., 139, 1911, 309–324.

§ Comptes Rendus, Paris, 52, 1861, 161, 212, 307, 817; Phil. Mag., 21, 1861, 136. Math. Papers, II, 229–235, 241, 262–3. Errors in early enunciations.

‖ Sitzungs. Ak. Wiss. Wien (Math.), 121, 1912, IIa, 589–592.

¶ Ibid., 727–742

H. S. Vandiver* applied the preceding theorems by Furtwängler and [23] to show that if Fermat's equation has integral solutions each prime to the exponent p and if $q(2) \not\equiv 0 \pmod{p^3}$, then $q(5) \equiv 0 \pmod{p}$ for $p \equiv 1 \pmod 3$, and $q(5) \equiv q(7) \equiv 0 \pmod{p}$ for $p \equiv 2 \pmod 3$.

Vandiver† applied [19], [20$_1$] and [23] to show that if Fermat's equation has integral solutions each prime to the exponent p,

$$q(5) \equiv 0, \qquad 1 + \tfrac{1}{2} + \tfrac{1}{3} + \cdots + \frac{1}{[p/5]} \equiv 0 \pmod{p}.$$

G. Frobenius‡ proved that if Fermat's equation has integral solutions each prime to the exponent p then $q(m)$ is divisible by p for $m = 11$ and $m = 17$ and, in case $p \equiv 5 \pmod 6$, also for $m = 7, 13, 19$. Moreover,

$$\sum_{l=1}^{m-1} \left\{ \frac{(l/m + h)^{p-1} - h^{p-1}}{p-1} \right\} x^l$$

vanishes identically modulo p for $m \leqq 22$ and $m = 24, 26$. Here the symbolic power h^λ is to be replaced by the Bernoullian number b_λ.

18. **Further papers on the function $q(m)$.** Eisenstein§ noted that

$$q(uv) \equiv q(u) + q(v), \qquad q(u + pv) \equiv q(u) - \frac{v}{u} \pmod{p},$$

$$2q(2) \equiv 1 - \tfrac{1}{2} + \tfrac{1}{3} - \cdots - \frac{1}{p-1} \equiv \frac{1}{(p-1)/2} + \cdots + \frac{1}{p-1} \pmod{p}.$$

J. Plana‖ set $S_i = 1^i + \cdots + (m-1)^i$ and proved that

$$m^j - m = jS_{j-1} + \binom{j}{2} S_{j-2} + \binom{j}{3} S_{j-3} + \cdots + jS_1.$$

M. A. Stern¶ set also $\sigma_i = 1^i + \cdots + m^i$ and proved that

$$\begin{aligned} \frac{m^p - m}{p} &\equiv S_1 - \tfrac{1}{2}S_2 + \cdots - \frac{1}{p-1} S_{p-1} \\ &\equiv \sigma_{p-1} + \tfrac{1}{2}\sigma_{p-2} + \cdots + \frac{1}{p-1}\sigma_1 \\ &\equiv \tfrac{1}{2}\left(\frac{m}{p-1} + \frac{m^2}{p-2} + \cdots + m^{p-1} \right) \\ &\qquad + \frac{1}{p-2} S_2 + \frac{1}{p-4} S_4 + \cdots + S_{p-1}, \end{aligned}$$

* Trans. Amer. Math. Soc., 15, 1914, 202–4.
† Jour. für Math., 144, 1914, 314–8.
‡ Sitzungs. Ak. Wiss. Berlin, 1914, 653–681.
§ Berlin Bericht, 1850, 41.
‖ Mem. Acad. Turin (2), 20, 1863, 120.
¶ Jour. für Math., 100, 1887, 182–8.

modulo p. Mirimanoff* proved the corrected form of Sylvester's formula. This was done also by J. W. L. Glaisher,† who‡ obtained other expressions for $q(m)$.

Lerch § treated at length $q(m)$ and $(a^{\phi(N)} - 1)/N$ for N composite. H. F. Baker‖ gave a formula for the latter quotient which generalizes Sylvester's. Friedmann and Tamarkine¶ gave formulas connecting $q(m)$ with Bernoullian numbers and with the greatest integer in m/p.

A. Cunningham** verified that $2^p - 2$ is not divisible by p^2 for any prime $p < 1000$, nor $3^p - 3$ by p^2 for a prime $p = 2^a \cdot 3^b + 1 < 100$.

W. Meissner†† gave the least residue of $(2^t - 1)/p$ modulo p for each prime $p < 2000$, where t is the exponent to which 2 belongs. The only case in which $2^p - 2$ is divisible by p^2 for $p < 2000$ is when $p = 1093$.

P. Bachmann‡‡ obtained expressions for $q(m)$.

H. S. Vandiver¶¶ proved that $q(2) \equiv 0 \pmod{p^2}$ if and only if

$$1 + \tfrac{1}{3} + \cdots + \frac{1}{p-2} \equiv 0 \pmod{p^2}.$$

* Jour. für Math., 115, 1895, 295–300.

† Quar. Jour. Math., 32, 1901, 1-27, 240–251.

‡ Messenger Math., 30, 1900–1, 78; Proc. London Math. Soc., 33, 1900–1, 49.

§ Math. Annalen, 60, 1905, 471–90; Comptes Rendus, Paris, 142, 1906, 35–8.

‖ Proc. London Math. Soc. (2), 4, 1906, 131–5.

¶ Jour. für Math., 135, 1909, 146–156.

** Report British Assoc., 1910, 530; l'intermédiaire des math., 18, 1911, 47; 19, 1912, 159; 20, 1913, 206.

†† Sitzungs. Ak. Berlin, 1913, 663–7.

‡‡ Jour. für Math., 142, 1913, 41–50.

¶¶ Annals of Math., Vol. 18, 1917, 112.

THE MODIFIED REMAINDERS OBTAINED IN FINDING THE HIGHEST COMMON FACTOR OF TWO POLYNOMIALS.

By A. J. Pell and R. L. Gordon.

E. B. Van Vleck* has shown how to simplify the computation of the remainders obtained in the process of finding the highest common factor of two polynomials: $a_0x^n + a_1x^{n-1} + \cdots + a_n$ and $b_0x^n + b_1x^{n-1} + \cdots + b_n$. The simplification consists in expressing the remainders as minors of a single determinant R (see page 163) which, on account of its construction, lends itself easily to computation. If the *first* coefficients of some of the remainders are zero, the results stated by Van Vleck must be modified. In this paper we determine by direct method the exact expression of the remainders.

In the derivation of this expression we need to transform two determinants some of whose rows are made up of elements which are two-rowed determinants. We give these transformations in the form of two lemmas, which are easy to prove.

Lemma 1. *If* λ *and* μ *are positive integers, and* $\gamma_i = \begin{vmatrix} \beta_0 & \beta_{i+1} \\ \alpha_0 & \alpha_{i+1} \end{vmatrix}$ *for* $i = 0, 1, \cdots, 2\lambda + \mu + 1$, *then*

$$\begin{vmatrix}
\gamma_0 & \gamma_1 & \gamma_2 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \gamma_{2\lambda+\mu+1} \\
\beta_0 & \beta_1 & \beta_2 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \beta_{2\lambda+\mu+1} \\
0 & \gamma_0 & \gamma_1 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \gamma_{2\lambda+\mu} \\
0 & \beta_0 & \beta_1 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \beta_{2\lambda+\mu} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & \gamma_0 & \gamma_1 & \gamma_2 & \cdots & \cdot & \cdot & \gamma_{\lambda+\mu+1} \\
0 & 0 & 0 & \cdots & \beta_0 & \beta_1 & \beta_2 & \cdots & \cdot & \cdot & \beta_{\lambda+\mu+1} \\
0 & 0 & 0 & \cdots & 0 & \beta_0 & \beta_1 & \cdots & \cdot & \cdot & \beta_{\lambda+\mu} \\
0 & 0 & 0 & \cdots & 0 & 0 & \beta_0 & \cdots & \cdot & \cdot & \beta_{\lambda+\mu-1} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \beta_0 & \cdots & \beta_{\lambda+1}
\end{vmatrix}$$

* E. B. Van Vleck, "On the determination of a series of Sturm's functions by the calculation of a single determinant," *Annals of Mathematics*, 1899, pp. 1–13.

$$= (-1)^{\lambda+1}\beta_0^{\lambda}\begin{vmatrix}
\alpha_0 & \alpha_1 & \alpha_2 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha_{2\lambda+\mu+2} \\
\beta_0 & \beta_1 & \beta_2 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \beta_{2\lambda+\mu+2} \\
0 & \alpha_0 & \alpha_1 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha_{2\lambda+\mu+1} \\
0 & \beta_0 & \beta_1 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \beta_{2\lambda+\mu+1} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \cdot & \cdot & \alpha_{\lambda+\mu+2} \\
0 & 0 & 0 & \cdots & \beta_0 & \beta_1 & \beta_2 & \cdots & \cdot & \cdot & \beta_{\lambda+\mu+2} \\
0 & 0 & 0 & \cdots & 0 & \beta_0 & \beta_1 & \cdots & \cdot & \cdot & \beta_{\lambda+\mu+1} \\
0 & 0 & 0 & \cdots & 0 & 0 & \beta_0 & \cdots & \cdot & \cdot & \beta_{\lambda+\mu} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \beta_0 & \cdots & \beta_{\lambda+1}
\end{vmatrix}.$$

LEMMA 2. *If* λ *and* μ *are positive integers,* $\begin{vmatrix} \beta_0\beta_i \\ \alpha_0\alpha_i \end{vmatrix} = 0$ *for* $i = 1, 2, \cdots, \mu - 1$, *and* $\gamma_{i-\mu} = \begin{vmatrix} \beta_0\beta_i \\ \alpha_0\alpha_i \end{vmatrix}$ *for* $i = \mu, \mu + 1, \cdots, 2\lambda + 2\mu + 1$, *then*

$$\begin{vmatrix}
\gamma_0 & \gamma_1 & \gamma_2 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \gamma_{2\lambda+\mu+1} \\
\beta_0 & \beta_1 & \beta_2 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \beta_{2\lambda+\mu+1} \\
0 & \gamma_0 & \gamma_1 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \gamma_{2\lambda+\mu} \\
0 & \beta_0 & \beta_1 & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \beta_{2\lambda+\mu} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & \gamma_0 & \gamma_1 & \gamma_2 & \cdots & \cdot & \cdot & \gamma_{\lambda+\mu+1} \\
0 & 0 & 0 & \cdots & \beta_0 & \beta_1 & \beta_2 & \cdots & \cdot & \cdot & \beta_{\lambda+\mu+1} \\
0 & 0 & 0 & \cdots & 0 & \gamma_0 & \gamma_1 & \cdots & \cdot & \cdot & \gamma_{\lambda+\mu} \\
0 & 0 & 0 & \cdots & 0 & 0 & \gamma_0 & \cdots & \cdot & \cdot & \gamma_{\lambda+\mu-1} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \gamma_0 & \cdots & \gamma_{\lambda+1}
\end{vmatrix}$$

$$= (-1)^{\mu(\lambda+1)}(-1)^{1+2+\cdots+\mu}\beta_0^{\lambda+1}\begin{vmatrix}
\alpha_0 & \alpha_1 & \alpha_2 & \cdots & \cdot & \cdot & \alpha_{2\lambda+2\mu+1} \\
\beta_0 & \beta_1 & \beta_2 & \cdots & \cdot & \cdot & \beta_{2\lambda+2\mu+1} \\
0 & \alpha_0 & \alpha_1 & \cdots & \cdot & \cdot & \alpha_{2\lambda+2\mu} \\
0 & \beta_0 & \beta_1 & \cdots & \cdot & \cdot & \beta_{2\lambda+2\mu} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & \alpha_0 & \cdots & \alpha_{\lambda+\mu+1} \\
0 & 0 & 0 & \cdots & \beta_0 & \cdots & \beta_{\lambda+\mu+1}
\end{vmatrix}.$$

The following theorem gives the exact expression of the remainders in terms of the minors of R, where

$$R = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ b_0 & b_1 & b_2 & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} & a_n & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{n-2} & b_{n-1} & b_n & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & a_2 & \cdots & a_n \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & b_2 & \cdots & b_n \end{vmatrix},$$

Theorem. Let

(A) $$a_0x^n + a_1x^{n-1} + \cdots + a_n,$$

and

(B) $$b_0x^n + b_1x^{n-1} + \cdots + b_n$$

be two polynomials of the nth degree. Modify the process of finding the highest common factor of (A) and (B) by taking at each stage the negative of the remainder. Let the ith modified remainder be

$R^{(i)}$ $$r_0^{(i)}x^{m_i} + r_1^{(i)}x^{m_i-1} + \cdots + r_{m_i}^{(i)},$$

*where $(m_i + 1)$ is the degree of the preceding remainder, and where the first $(p_i - 1)$ coefficients of $R^{(i)}$ are zero, and the p_ith coefficient $\rho_i = r_{p_i-1}^{(i)}$ is different from zero. Then for $k = 0, 1, \cdots, m_i$, the coefficients $r_k^{(i)}$ are given by**

(1) $$r_k^{(i)} = \frac{(-1)^{u_{i-1}}(-1)^{u_{i-2}} \cdots (-1)^{u_1}(-1)^{v_{i-1}}}{\rho_{i-1}^{p_{i-1}+1}\rho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \rho_1^{p_1+p_2}\rho_0^{p_1}}$$

$$\times \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & \cdot & \cdot & \cdot & a_{2v_{i-1}} & a_{2v_{i-1}+1+k} \\ b_0 & b_1 & b_2 & \cdots & \cdot & \cdot & \cdot & b_{2v_{i-1}} & b_{2v_{i-1}+1+k} \\ 0 & a_0 & a_1 & \cdots & \cdot & \cdot & \cdot & a_{2v_{i-1}-1} & a_{2v_{i-1}+k} \\ 0 & b_0 & b_1 & \cdots & \cdot & \cdot & \cdot & b_{2v_{i-1}-1} & b_{2v_{i-1}+k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_{v_{i-1}} & a_{v_{i-1}+1+k} \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_{v_{i-1}} & b_{v_{i-1}+1+k} \end{vmatrix},$$

where $u_{i-1} = 1 + 2 + \cdots + p_{i-1}$, and $v_{i-1} = p_1 + p_2 + \cdots + p_{i-1}$.

Divide (A) by (B) and the remainder with sign changed may be expressed as follows:

* It is to be understood in (1) that $\rho_0 = b_0$, $p_0 = 0$, and that $a_i = b_i = 0$ for $i > n$.

$$R^{(1)} = \frac{1}{b_0}\left\{ \begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix} x^{n-1} + \begin{vmatrix} a_0 & a_2 \\ b_0 & b_2 \end{vmatrix} x^{n-2} + \cdots + \begin{vmatrix} a_0 & a_n \\ b_0 & b_n \end{vmatrix} \right\}.$$

Hence the coefficients of $R^{(1)}$ satisfy (1) for $i = 1$.

Suppose that (1) is true for $i = l$, then it follows that

$$(2)\quad r_k^{(l+1)} = \frac{(-1)^{u_l}(-1)^{u_{l-1}} \cdots (-1)^{u_2}(-1)^{v_l - p_1}}{\rho_l^{p_1+1}\rho_{l-1}^{p_{l-1}+p_l} \cdots \rho_2^{p_2+p_3}\rho_1^{p_2}}$$

$$\times \begin{vmatrix} \bar{s}_0 & \bar{s}_1 & \cdots & \cdots & \bar{s}_{2v_l-2p_1} & \bar{s}_{2v_l-2p_1+1+k} \\ r^{(1)}_{p_1-1} & r^{(1)}_{p_1} & \cdots & \cdots & r^{(1)}_{2v_l-p_1-1} & r^{(1)}_{2v_l-p_1+k} \\ \cdot & \cdot & \cdots & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots 0 & \bar{s}_0 \cdots & \bar{s}_{v_l-p_1} & \bar{s}_{v_l-p_1+1+k} \\ 0 & 0 & \cdots 0 & r^{(1)}_{p_1-1} \cdots & r^{(1)}_{v_l-1} & r^{(1)}_{v_l+k} \end{vmatrix},$$

where the $\bar{s}_i$ are the coefficients of the remainder of the next to the last stage in dividing B by $R^{(1)}$. The $\bar{s}_i$ may be expressed as two-rowed determinants:

$$\bar{s}_i = \frac{1}{\rho_1}\begin{vmatrix} r^{(1)}_{p_1-1} & r^{(1)}_{i+p_1} \\ \bar{s}_0 & \bar{s}_{i+1} \end{vmatrix},$$

and hence Lemma 1 may be applied to the determinant in (2), where $\lambda = v_l - p_1$ and $\mu = 0$. A determinant of the same character as in (2) is obtained, for the $\bar{s}_i$ are also expressible as $1/\rho_1$ times two-rowed determinants:

$$\bar{s}_i = \frac{1}{\rho_1}\begin{vmatrix} r^{(1)}_{p_1-1} & r^{(1)}_{i+p_1} \\ \bar{s}_0 & \bar{s}_{i+1} \end{vmatrix}.$$

Lemma 1 may be applied again, with $\lambda = v_l - p_1$ and $\mu = 1$. The process may be repeated, and after applying Lemma 1 p_1 times,* a determinant in terms of b_i and $r_i^{(1)}$ is obtained. The factor outside the determinant becomes multiplied by

$$\left(\frac{(-1)^{v_l-p_1+1}\rho_1^{v_l-p_1}}{\rho_1^{v_l-p_1+1}}\right)^{p_1},$$

and the determinant for $r_k^{(l+1)}$ takes the form

* Some of the partial quotients may be zero, that is, the first elements in some sets of s's may be zero. In that case the elements of one set of s's are equal to the elements of the next set, with the subscripts advanced by one.

$$
(3)\qquad
\begin{vmatrix}
b_0 & b_1 & b_2 & \cdots & \cdots & b_{2v_l-2p_1+1} & b_{2v_l-2p_1+2+k} \\
r_{p_1-1}^{(1)} & r_{p_1}^{(1)} & r_{p_1+1}^{(1)} & \cdots & \cdots & r_{2v_l-p_1}^{(1)} & r_{2v_l-p_1+1+k}^{(1)} \\
0 & b_0 & b_1 & \cdots & \cdots & b_{2v_l-2p_1} & b_{2v_l-2p_1+1+k} \\
0 & r_{p_1-1}^{(1)} & r_{p_1}^{(1)} & \cdots & \cdots & r_{2v_l-p_1-1}^{(1)} & r_{2v_l-p_1+k}^{(1)} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & b_{v_l-p_1+1} & b_{v_l-p_1+2+k} & \\
0 & 0 & 0 & \cdots & r_{p_1-1}^{(1)} & r_{v_l}^{(1)} & r_{v_l+1+k}^{(1)} \\
0 & 0 & 0 & \cdots & 0 & r_{v_l-1}^{(1)} & r_{v_l+k}^{(1)} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & 0 & r_{v_l-p_1}^{(1)} & r_{v_l-p_1+1+k}^{(1)}
\end{vmatrix}.
$$

Now, $r_i^{(1)} = 0$ for $i = 0, 1, \cdots, (p_i - 2)$, and

$$
r_i^{(1)} = -\frac{1}{b_0}\begin{vmatrix} b_0 & b_{i+1} \\ a_0 & a_{i+1} \end{vmatrix}
$$

for $i = p_1 - 1, p_1, \cdots$, so that if each pair of two consecutive b_i and $r_i^{(1)}$ rows in (3) are interchanged, a determinant of the form in Lemma 2 is obtained. Hence Lemma 2 may be applied with $\lambda = v_l - p_1$ and $\mu = p_1$. The result is that the factor outside the determinant is multiplied by

$$
\frac{(-1)^{v_l-p_1+1}(-1)^{p_1(v_l-p_1+1)}(-1)^{u_1}\rho_0^{\,v_l-p_1+1}}{(-\rho_0)^{v_l+1}}
$$

and the determinant becomes one with $p_l + p_{l-1} + \cdots + p_1 + 1$ pairs of a_i and b_i rows. After simplifying the outside factor the following is obtained:

$$
r_k^{(l+1)} = \frac{(-1)^{u_l}(-1)^{u_{l-1}}\cdots(-1)^{u_1}(-1)^{v_l}}{\rho_l^{\,p_l+1}\rho_{l-1}^{\,p_{l-1}+p_l}\cdots\rho_1^{\,p_1+p_2}\rho_0^{\,p_1}}
$$

$$
\times
\begin{vmatrix}
a_0 & a_1 & a_2 & \cdots & \cdots & a_{2v_l} & a_{2v_l+1+k} \\
b_0 & b_1 & b_2 & \cdots & \cdots & b_{2v_l} & b_{2v_l+1+k} \\
0 & a_0 & a_1 & \cdots & \cdots & a_{2v_l-1} & a_{2v_l+k} \\
0 & b_0 & b_1 & \cdots & \cdots & b_{2v_l-1} & b_{2v_l+k} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots a_0 & a_1 \cdots & a_{v_l} & a_{v_l+1+k} \\
0 & 0 & 0 & \cdots b_0 & b_1 \cdots & b_{v_l} & b_{v_l+1+k}
\end{vmatrix}.
$$

This is the form of (1) for $i = l + 1$, and the theorem is proved.

In case $b_0 > 0$, and $p_i = 1$ for $i = 1, 2, \cdots, n$, that is, when the first

coefficients of all the remainders are different from zero, the factor outside the determinant is positive, and the coefficients of the ith remainder are given except for the positive factor by the minors of R formed from the first $2i$ rows by associating the elements in the first $2i - 1$ columns with each of the other columns. This is the rule which Van Vleck* gives as holding for any case, but if, for example, $p_1 = 2$, the coefficients of the second modified remainder $R^{(2)}$ are given by the 6-rowed minors formed from the first 6 rows of R, and the sign factor is

$$\frac{(-1)^{1+2}(-1)^2}{b_0^2 \rho_1^3},$$

which is negative if ρ_1 is positive.

If (A) is of degree n, and (B) of degree $n - p_0$, the coefficients of the ith modified remainder

$$R^{(i)} \qquad r_0^{(i)} x^{m_i} + r_1^{(i)} x^{m_i - 1} + \cdots + r_{m_i}^{(i)}$$

are given for $k = 0, 1, 2, \cdots, m_i$, by

$$r_k^{(i)} = \frac{(-1)^{r_{i-1}}(-1)^{u_{i-1}}(-1)^{u_{i-2}} \cdots (-1)^{u_0}(-1)^{(p_0/2)2r_{i-1}-p_0+1)}}{\rho_{i-1}^{p_{i-1}+1}\, \rho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \rho_1^{p_1+p_2}\, \rho_0^{p_0+p_1}}$$

$$\times \begin{vmatrix}
a_0 & a_1 & a_2 & \cdots & \cdot & \cdot & \cdot & \cdot & a_{2r_{i-1}-p_0} & a_{2r_{i-1}-p_0+1+k} \\
b_0 & b_1 & b_2 & \cdots & \cdot & \cdot & \cdot & \cdot & b_{2r_{i-1}-p_0} & b_{2r_{i-1}-p_0+1+k} \\
0 & a_0 & a_1 & \cdots & \cdot & \cdot & \cdot & \cdot & a_{2r_{i-1}-p_0-1} & a_{2r_{i-1}-p_0+k} \\
0 & b_0 & b_1 & \cdots & \cdot & \cdot & \cdot & \cdot & b_{2r_{i-1}-p_0-1} & b_{2r_{i-1}-p_0+k} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_{r_{i-1}} & a_{r_{i-1}+1+k} & \\
0 & 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_{r_{i-1}} & b_{r_{i-1}+1+k} & \\
0 & 0 & 0 & \cdots & 0 & b_0 & \cdots & b_{r_{i-1}-1} & b_{r_{i-1}+k} & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & 0 & \cdots & b_0 & \cdots & b_{r_{i-1}-p_0} & b_{r_{i-1}-p_0+1+k}
\end{vmatrix},$$

where $u_i = 1 + 2 + \cdots + p_i$ and $v_i = p_0 + p_1 + \cdots + p_i$.

* L. c., pp. 3, 4.

MT. HOLYOKE COLLEGE.

NOMOGRAMS OF ADJUSTMENT.*

By L. I. Hewes.

D'Ocagne has shown† that any equation of the form

$$\begin{vmatrix} f_1 & g_1 & 1 \\ f_2 & g_2 & 1 \\ f_3 & g_3 & 1 \end{vmatrix} = 0, \tag{1}$$

where f_i and g_i are any functions of one variable, may be represented by a collinear nomogram or diagram of alignment. For this purpose it is only necessary to set up the three pairs of defining equations‡

$$x = f_i, \quad y = g_i \qquad (i = 1, 2, 3),$$

and plot the three corresponding curves which are inscribed with the values of the corresponding parameters z_i. A graphical solution for any unknown z_i is then found by applying a straight edge or index through two known values of z_i.

This procedure has also been extended to include equations of the type

$$\begin{vmatrix} f_{12} & g_{12} & 1 \\ f_{34} & g_{34} & 1 \\ f_{56} & g_{56} & 1 \end{vmatrix} = 0, \tag{2}$$

where the equations

$$x = f_{ij}, \quad y = g_{ij} \qquad (i = 1, 3, 5;\ j = 2, 4, 6)$$

define in general three curve nets.

It is observed that in equations (1) and (2) the variables z are so segregated that any one of them appears in but one row of the determinant. The class of equations to which the theory is applicable is consequently restricted. It is proposed to remove this particular restriction from equation (1), and from equation (2) when the number of vari-

* Read by title at the Cambridge Summer Meeting of the American Mathematical Society, Sept. 5, 1916.

† Traité de Nomographie, Paris, 1899, Ch. III, and Ch. V, and Calcul Graphique et Nomographie, Paris, 1908, Ch. IV.

‡ Indicated by d'Ocagne, l. c., and adopted by Soreau, "Contribution à la théorie . . . de la Nomographie," Mém. et comptes rendus de la Soc. des Ing. civils, 1901.

ables does not exceed five, by introducing the additional principle of *adjustment of the index.*

Consider first equations of the form

$$\begin{vmatrix} f_{ij} & g_{ij} & 1 \\ f_{kl} & g_{kl} & 1 \\ f_{mn} & g_{mn} & 1 \end{vmatrix} = 0, \tag{3}$$

where the subscripts denoting the variables are allowed to take on in pairs *any* values from the set of numbers 0, 1, 2, 3 with the understanding that 0 shall denote the absence of a second variable in any function. Upon setting up the defining equations

$$x = f_{ij}, \quad y = g_{ij},$$

$$x = f_{kl}, \quad y = g_{kl},$$

$$x = f_{mn}, \quad y = g_{mn},$$

it is seen that the corresponding geometric configuration in the plane, in the most general case, consists of three curve nets and that when any two nets are considered there always appears one family of curves in each in which the curves correspond to the *same* parameter z. In general three collinear points found respectively in the three nets will not yield values of the parameters z attached to the corresponding pairs of curves intersecting at the points, which are solutions of equation (3), but six unrelated values of the parameters z_1, z_2, z_3. When however six curves, which are inscribed with values of z_1, z_2, z_3, which constitute a solution of equation (3) are selected in the three nets, it is at once evident from the defining equations of equation (3) that the six curves intersect in pairs at points which are collinear. It remains therefore to establish a method for the converse process.

In practice one variable only is unknown, therefore there will always be one curve net in the most unfavorable case in which a point is determined by the values of the two knowns. In each of the remaining two nets one curve is known. Therefore if the index is rotated about the given point until its intersections with the two known curves are at points on curves inscribed with the *same* value of the unknown, that value of the unknown z is the value sought.

There are eight distinct cases of equation (3) if all trivial cases are excluded. These eight cases have the following determinants for the left-hand member:

$$\text{I.}\quad \begin{vmatrix} f_1 & g_1 & 1 \\ f_2 & g_2 & 1 \\ f_3 & g_3 & 1 \end{vmatrix}, \quad \text{II.}\quad \begin{vmatrix} f_1 & g_1 & 1 \\ f_2 & g_2 & 1 \\ f_{13} & g_{13} & 1 \end{vmatrix}, \quad \text{III.}\quad \begin{vmatrix} f_1 & g_1 & 1 \\ f_{12} & g_{12} & 1 \\ f_{13} & g_{13} & 1 \end{vmatrix}, \quad \text{IV.}\quad \begin{vmatrix} f_1 & g_1 & 1 \\ f_{12} & g_{12} & 1 \\ f_{23} & g_{23} & 1 \end{vmatrix},$$

$$\text{V.}\quad \begin{vmatrix} f_{12} & g_{12} & 1 \\ f_{13} & g_{13} & 1 \\ f_{23} & g_{23} & 1 \end{vmatrix}, \quad \text{VI.}\quad \begin{vmatrix} f_1 & g_1 & 1 \\ f_{23} & g_{23} & 1 \\ f_{23} & g_{23} & 1 \end{vmatrix}, \quad \text{VII.}\quad \begin{vmatrix} f_{12} & g_{12} & 1 \\ f_{13} & g_{13} & 1 \\ f_{13} & g_{13} & 1 \end{vmatrix}, \quad \text{VIII.}\quad \begin{vmatrix} f_1 & g_1 & 1 \\ f_1 & g_1 & 1 \\ f_{23} & g_{23} & 1 \end{vmatrix}.$$

It is seen that in cases III and VII it is possible that the unknown variable may enter in each row in which case no initial fixed point would be determined and the position of the index which yields a solution would only be found by trial and error. On the other hand in these same two cases if the variable entering each row is known there is no adjustment of the index required.* Nor is adjustment required in several other cases, *e. g.*, II when z_3 is unknown, etc. Case I is of course d'Ocagne's equation of three variables.

In many examples in practice one (or more) of the functions reduces to a constant in which event d'Ocagne's notion of a binary scale† is needed in carrying out the construction unless the other function in the corresponding row contains but one variable; in that case only a straight scale is involved. If the unknown value is involved in the net of the binary scale the management of the index becomes troublesome unless a known value enters in each row of the determinant.

As an application of the above theory consider the equation

$$z_1 z_2 - z_3 + \sqrt{1 + z_2^2}\sqrt{1 + z_1^2} = 0,$$

which d'Ocagne has pointed out‡ cannot be written in the form (1) above. This equation is however of the type VIII of equation (3). It may be written in the determinant form

$$(4) \qquad \begin{vmatrix} 1 & z_1 & 1 \\ 0 & \sqrt{1 + z_1^2} & 1 \\ \dfrac{z_2}{z_2 + \sqrt{1 + z_2^2}} & \dfrac{z_3}{z_2 + \sqrt{1 + z_2^2}} & 1 \end{vmatrix} = 0.$$

* Unless z_3 is unknown in case VII.

† L. c., Ch. V and Ch. III respectively.

‡ L. c., pp. 419–22 and pp. 185 and 229 respectively.

The corresponding defining equations are

$$x = 1, \qquad y = z_1,$$

$$x = 0, \qquad y = \sqrt{1 + z_1^2},$$

$$x = \frac{z_2}{z_2 + \sqrt{1 + z_2^2}}, \qquad y = \frac{z_3}{z_2 + \sqrt{1 + z_2^2}}.$$

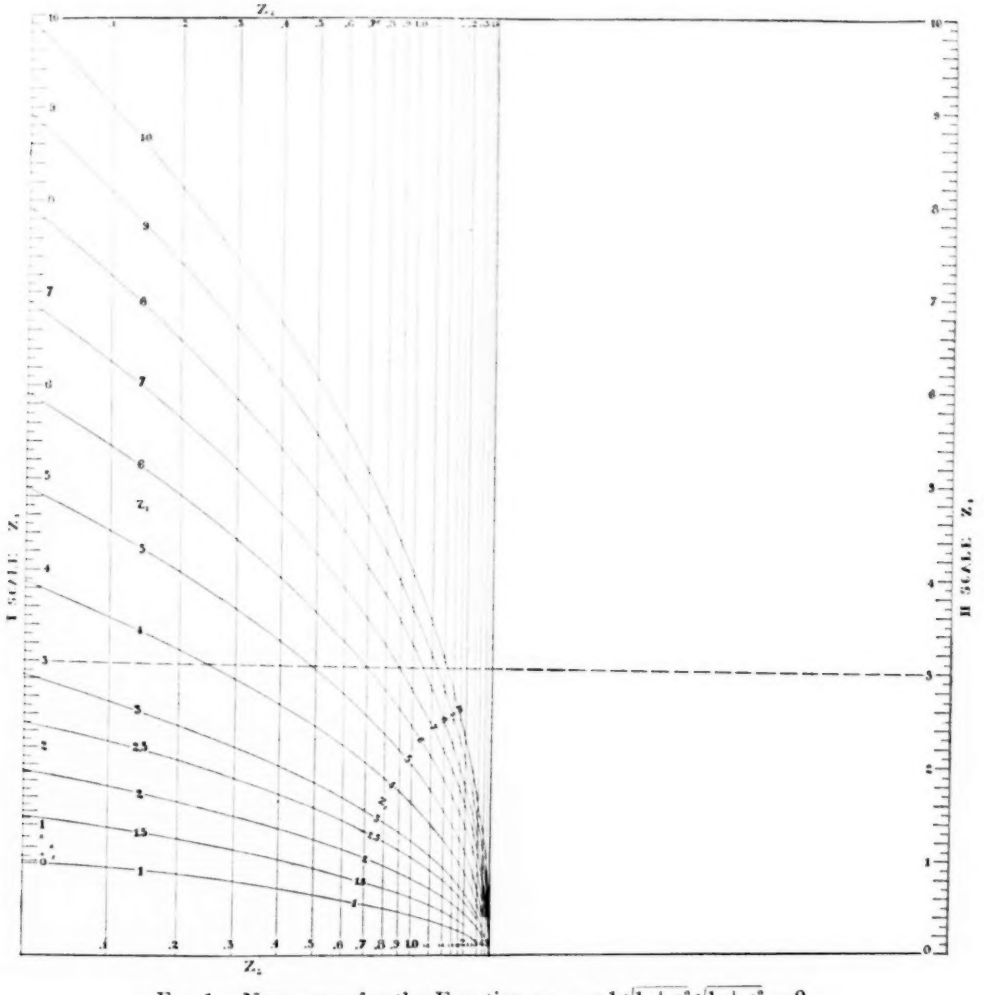


FIG. 1. Nomogram for the Equation $z_2 z_3 - z_1 1 \sqrt{1 + z^2} \sqrt{1 + z^2} = 0$.

Since z_1 appears only in g_1 the first two scales for z_1 are straight scales on the lines $x = 1$ and $x = 0$. The net of curves for z_2 and z_3 consists of lines parallel to the y- axis inscribed with values of z_2 and the family of

parabolas

$$y^2 = z_3^2(1 - 2x)$$

and inscribed with corresponding values of z_3. The finished diagram is shown in Fig. 1. If z_1 is known, no adjustment of the index is required but if it is unknown then the index must be rotated about the point determined by z_2 and z_3 in the net until the intersections with the two straight scales yield the same value.

By analogy with the class of equations (3) equations of more than three variables may be represented by nomograms in which corresponding geometric elements appear more than once. The equation

$$\begin{vmatrix} f_{ij} & g_{ij} & 1 \\ f_{kl} & g_{kl} & 1 \\ f_{mn} & g_{mn} & 1 \end{vmatrix} = 0, \tag{5}$$

where the subscripts are allowed to take on any two different values in pairs from the numbers 0, 1, 2, 3, 4, and 5, exhausts all possible cases.

An example of equation (5) is afforded by the bi-quadratic equation

$$z^4 + a_1z^3 + a_2z^2 + a_3z + a_4 = 0,$$

which may be written in the determinant form

$$\begin{vmatrix} -z & a_4 + z^4 & 1 \\ \dfrac{a_2}{a_1} & \dfrac{a_2}{a_1}a_3 & 1 \\ 0 & -a_2z^2 & 1 \end{vmatrix} = 0,$$

and the quotient of the two coefficients a_2/a_1 may be regarded as a single variable parameter k. The only calculation involved in the solution is then to determine this quotient. The nomogram is constructed from the defining equations

$$x = -z, \quad y = a_4 + z^4,$$

$$x = \frac{a_2}{a_1}, \quad y = \frac{a_2}{a_1}a_3,$$

$$x = 0, \quad y = -a_2z^2,$$

and it is necessary to have a binary scale on the line $x = 0$ for which the segregation of the variables a_2 and z is accomplished by setting $x = -z$ in order to take advantage of the z lines already required in the first net. The nomogram is entered with the value of the parameter k and the

coefficient a_3 which determine a point in the second curve net. The index must then be rotated until it intersects the proper a_4 curve at a point with the same abscissa as the point of intersection of the parabola

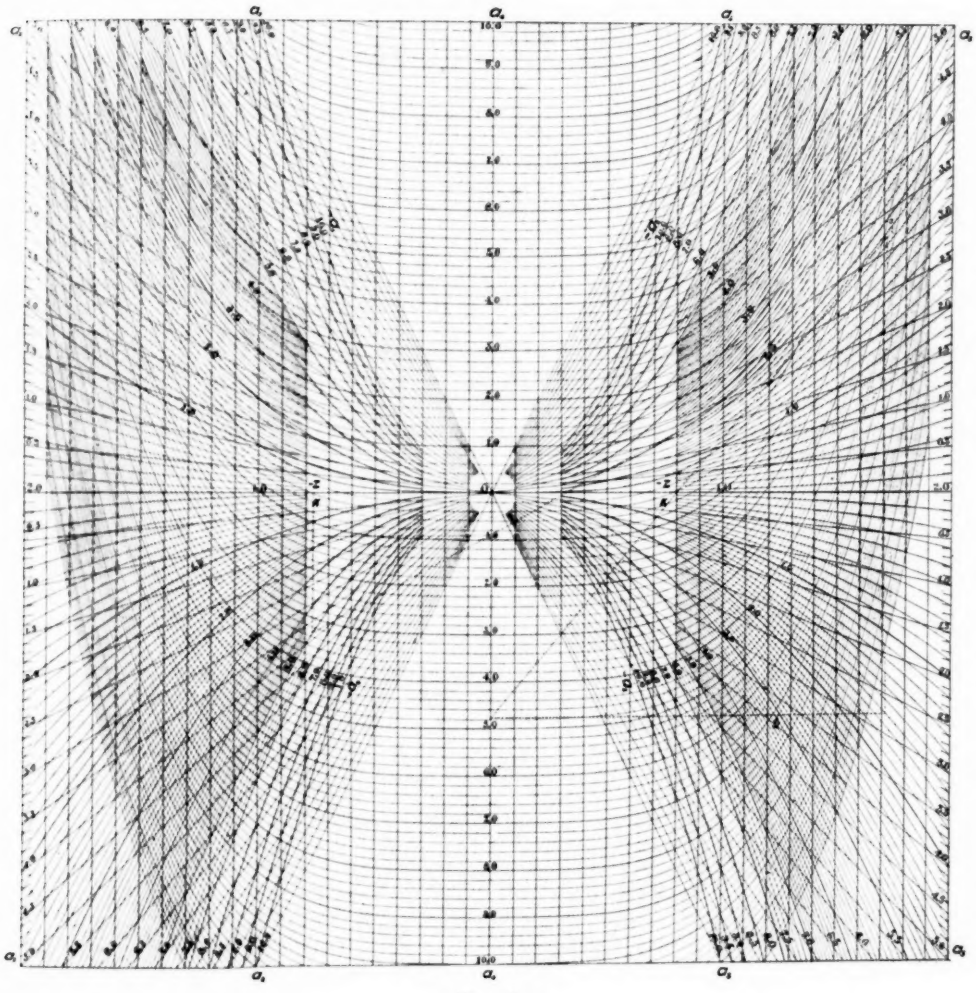


FIG. 2.

a_2 and the horizontal projecting line from the point of intersection of the index with the Y axis. In the figure the index is set for the two real roots of the bi-quadratic equation

$$z^4 + 1.33z^3 + 1.6z^2 + 2z - 3.3 = 0.$$

FAIRFAX COUNTY, VA.,
September 9, 1916.

CLOSED ALGEBRAIC CORRESPONDENCES.

By Albert A. Bennett.

Correspondences and their Reducibility.

1. Let M be a complex algebraic manifold of one dimension. We may regard M either as a complex curve in a space in which the curve is without multiple points, or we may think of M abstractly as a Riemann surface not only without multiple points but without recognizable branch points and points "at infinity." We shall use the letters $x, y, \cdots$, to denote representative points on the manifold, although, of course, it is impossible to identify a point of M by means of a single *rational* parameter except when M is itself rational. We shall write $C(x, y)$ as the symbol* of an algebraic correspondence on M, by which for any given point x of M, there are algebraically determined n points y of M, in general distinct, regarded as corresponding to x, all of which vary as x varies, and conversely, for any given y, there are determined algebraically m points x of M, in general distinct, each of which yields the given y by means of the correspondence, and each of which varies with y. These numbers, m and n, which are called the *orders* of the correspondence, may be brought more explicitly into evidence by writing the symbol in the form $C(\overset{m}{x}, \overset{n}{y})$. Any analytic correspondence with no essential singular points is readily seen to be of finite orders, or in other words, algebraic, cf. Hurwitz, l. c.

For a given x we obtain n and only n values of y by means of $C(x, y)$. We may let x make any desired circuit on M, but whenever x returns to its initial position, the set of values of y must return to its initial position. Permutations may however have occurred within the set. The totality of all permutations that can be obtained by means of closed circuits described by x will form a permutation group G of degree n but of order depending upon the correspondence. We may select an initial position ξ_0 for x, for which no two of the corresponding values of y coincide, and select for $x = \xi_0$ one of the points y which we shall call y_1. As x makes all types of closed circuits starting from ξ_0 and returning to it, it may or

* When in place of M, we take a plane curve defined by an equation $f(x_0, x_1, x_2) = 0$ where x_0, x_1, x_2 are homogeneous, there exist correspondences which can be defined as the common solution of two equations, $P_1(x_0, x_1, x_2;\ y_0, y_1, y_2) = 0$ and $P_2(x_0, x_1, x_2;\ y_0, y_1, y_2) = 0$ on $f(x_0, x_1, x_2) = 0$, but which cannot be expressed by means of a single equation $P(x_0, x_1, x_2; y_0, y_1, y_2) = 0$, on $f = 0$. Cf. Hurwitz, Math. Ann., 28, 561 ff. (1887).

may not happen that y_1 is carried into each of the other y's, that is, it may or may not happen that G is transitive. If G is non-transitive, then C is said to be *reducible* with respect to y, but otherwise, *irreducible* with respect to y. We may similarly define irreducibility with respect to x.

Addition and Multiplication of Correspondences.

2. We may consider certain methods of combining correspondences which may be denoted by addition and multiplication respectively.* Indeed, if $C_1(\overset{m}{x}, \overset{n}{y})$ be one given correspondence and $C_2(\overset{p}{x}, \overset{q}{y})$ be another, then by $C_3 = C_1 + C_2$, will be meant the correspondence $C_3(\overset{m+p}{x}, \overset{n+q}{y})$ obtained by regarding every point y corresponding to the x supposed given, whether by C_1 or by C_2 as corresponding to this x by C_3, and hence similarly with the x's yielding a given y. We may introduce the symbol, zero, 0, to stand for any "correspondence" which involves neither x nor y. Hence $C + 0 = 0 + C = C$. Further, $C_1 + C_2 = C_2 + C_1$, $C_1 + (C_2 + C_3) = (C_1 + C_2) + C_3$, or in other words, addition of correspondences is commutative and associative.

In an analogous manner we shall define the product $C_3 = C_1C_2$, as the correspondence $C_3(\overset{mp}{x}, \overset{nq}{y})$ obtained from C_1 and C_2 by starting with a given x and obtaining the n z's given by $C_1(\overset{m}{x}, \overset{n}{z})$ and then for each of these z's, finding the q y's given by $C_2(\overset{p}{z}, \overset{q}{y})$, and finally regarding these nq y's as the y's corresponding to the given x by C_3. This will also give us the mp x's for a given y obtained by considering the converse relationships. The correspondence given by $y = x$, will be the identity for multiplication and may be denoted by the symbol 1. The symbol aC^b, where a and b are given positive integers will now have a definite meaning for any given C. The distributive character of multiplication is readily verified.

If C_1 be a correspondence irreducible with respect to y and another different correspondence, C_2 be given such that as x varies, one of the points y obtained from x by C_1 is always obtainable from x also by C_2, then C_2 contains all of the points corresponding to x by C_1, since a suitable closed circuit of x will carry this common y into any other desired point y given by C_1.

If C^2 contains x we shall have an equation of the form

$$C^2 = a + C_1,$$

where a is a positive integer indicating the number of times C^2 contains x.

* Cf. Severi, Torino, Mem. (2), 54, 1 (1903).

If C^2 contains any point already given by C, we shall have

$$C^2 = bC + C_2,$$

where b is the number of times C^2 contains C. It often happens that there exists an integer k, such that C^k can be expressed entirely in terms of C's of lower powers. In such a case there are k integers, $a_1, a_2, \cdots, a_k$, such that

$$C^k = a_1C^{k-1} + a_2C^{k-2} + \cdots + a_{k-1}C + a_k.$$

These cases are particularly interesting as the C's can then give only a finite number of distinct points by any amount of addition and multiplication, and a sort of finite number system is constructed. For any C satisfying an equation of the above form, we must have the orders m and n, equal. For, in terms of the orders we have

$$m^k = a_1m^{k-1} + a_2m^{k-2} + \cdots + a_{k-1}m + a_k,$$
$$n^k = a_1n^{k-1} + a_2n^{k-2} + \cdots + a_{k-1}n + a_k.$$

Thus m and n would have to be, otherwise, distinct real positive roots of an equation which by Descartes' rule of signs can have at most one real positive root. Hence $m = n$. There exist, also, obvious restrictions upon the integer coefficients a_i, $i = 1, 2, \cdots, k$ if there is to be a solution m for the order of the correspondence.

Closed Correspondences on an Algebraic Manifold M.

3. We have mentioned a type of case in which the total number of points obtained from a variable point x, by means of $C(x, y)$ is finite. We shall introduce the more general notion of a closed system as follows: If a correspondence $C(x, y)$ be such that starting from a variable point x, the maximum number of distinct points given by any correspondence of the form, $1 + C + C^2 + \cdots + C^h$ is finite and equal to ν, no matter how great h be taken, nor how x varies over the manifold M, then C is said to generate a closed system.

Let us suppose we have generated a closed system S of ν points on M. These ν points will form a one-parameter involution of index one,* since the entire system as a whole, although not the relative positions of the points among themselves, is fixed uniquely by the position on M of any point of the set, without regard to distinctions among the points. We shall now examine some properties of this type of involution.

We are given a set of ν variable points, among which there will be, in particular, a permutation group G' consisting of the permutations of the remaining $\nu - 1$ points, which arise when a selected point varies over

* Enriques, Rend. Circ. M. Palermo, 10, 30 (1895).

closed circuits on M. This group will be independent of the particular variable point selected and of the fixed position ξ_0 on M from which this variable point starts out and to which it returns, provided only that at most a finite number of special points which serve as branch points for the group be excluded from M. Let μ be the order of G'. Let x be a point of S, and let $r_1, r_2, \cdots, r_e$ be a set of independent rational functions of x and of the remaining $\nu - 1$ points of S, these functions being unsymmetric in the points of S. The value of r_i, $i = 1, 2, \cdots, e$, will not be determined by x alone but will have μ different determinations for a given position of x, corresponding to the permutations of the remaining points of S. In any given case we may take e sufficiently large so that the values of the e r's being known, the point x is completely determined, although in every case x will determine μ sets of values of the r's. By using the r's as the parameters of a point in e-space, we define a one-dimensional algebraic manifold M' such that each point x of M determines algebraically μ points of M' in general distinct, and each point of M' is obtained from but a single point of M. We may then regard M' as mapped as a μ-sheeted Riemann surface upon M.

A One-to-One Reciprocal Correspondence Group on the Associated Manifold M'.

4. Let the ν points of the involution S on M, be numbered arbitrarily as, $x_1, x_2, \cdots, x_\nu$, and let the μ points of M' corresponding to the point x_i of M, be numbered arbitrarily as $x_{i1}, x_{i2}, \cdots, x_{i\mu}$. Then if we observe that a point, for example, x_{11}, of M' corresponds not merely to a point, viz., x_1, of M, but also to a definite permutation among the other points, $x_2, x_3, \cdots, x_\nu$, of M, we see that whenever the point x_{11}, describes a closed circuit, each of the points, $x_1, x_2, \cdots, x_\nu$, and therefore also each of the sets $(x_{i1}, x_{i2}, \cdots, x_{i\mu})$, $i = 1, 2, \cdots, \nu$, is transformed into itself. Moreover since the points, $x_1, x_2, \cdots, x_\nu$, of the involution are not permuted, and since the points within a set $(x_{i1}, x_{i2}, \cdots, x_{i\mu})$, correspond to the different permutations among the points of the involution, the points within a set $(x_{i1}, x_{i2}, \cdots, x_{i\mu})$ are also carried individually into themselves. Let S' be the set of variable points x_{ij} on M', $\mu\nu$ in number. The correspondence on M' between any one point of S' and any other is therefore not only algebraic but actually one to one reciprocally. Hence S' consists of a set of points obtained by a group of one-to-one correspondences on M', and M' admits of a group of algebraic one-to-one reciprocal correspondences into itself.

Conditions upon Correspondences which Generate Closed Systems.

5. Interpreted algebraically, the connected surface M' which is μ-sheeted with respect to M, determines an irreducible algebraic irrationality

A on M, such that given any point x of M, $x' = A(x)$ is an irreducible μ-valued algebraic function of x, whose array of values may be used to construct M' upon M. We may indicate the μ determinations of A by subscripts, thus $A_j(x)$, $j = 1, 2, \cdots, \mu$ although two of these determinations may be permuted by a closed circuit on M. Given x and an associated value of x', we have always but a single point of M' determined. The fact that all the points x_{ij} vary over the same manifold M' is equivalent to saying that given any x_{ij}, that is given x_i and its associated $x_{ij}' = A_j(x_i)$ any other $x_{i'j'}$ is birationally determined, that is both $x_{i'}$ and its associated $x'_{i'j'} = A_{j'}(x_{i'})$ are birationally determined.

In terms of the original correspondence $C(x, y)$, this gives us the following: A necessary condition that a correspondence $C(x, y)$, irreducible with respect to y, can generate a closed system is that there exist on M, an irreducible algebraic μ-valued function A, such that given x and any desired determination of $A(x)$, say x', each y satisfying $C(x, y)$ together with each associated $y' = A(y)$ is obtainable rationally, while this pair of values, (y, y'), also determine x and x', rationally. We may represent $C(x, y)$ symbolically by a set of equations of the type,

$$y = \varphi_1(x, x'), \qquad x = \psi_1(y, y'),$$
$$y' = \varphi_2(x, x'), \qquad x' = \psi_2(y, y'),$$

where φ_1, φ_2, ψ_1, ψ_2, are all rational for $x' = A(x)$, and $y' = A(y)$.

If M' is of genus greater than one, which often happens when the genus of M is zero or one, and always when the genus of M is greater than one, the above condition is also sufficient, since in this case the entire system of points will be generated by a group of one-to-one reciprocal correspondences on a one-dimensional algebraic manifold, which is in every instance a finite group.* For M' of genus zero or one, we must introduce additional conditions of closure if the set is required to be finite. These conditions are algebraically expressible, but occur very naturally as linear relations among rational or elliptic functions according as M' is of genus zero or one. The best known examples are furnished by the closure conditions for Poncelet and Steiner polygons.†

* Various numerical relations between the genera of manifolds related as M and M' are known. Cf., e. g., Zeuthen, Lehrbuch der abzählenden Methoden der Geometrie, Chap. IV, Teubner, 1914. That the group of transformations for a genus greater than one is finite was proved most elegantly, perhaps, by Hurwitz, Math. Ann., 32 and 41, but many earlier and later proofs have been made. Cf. Pascal, Repertorium, II, 1, 2d ed., p. 352.

† For an explicit algebraic discussion and derivation of the algebraic conditions, cf. "An algebraic treatment of the theorem of closure," by the author, *Annals of Mathematics* (16), p. 96 (1915).

Groups Associated with Closed Correspondences.

6. The system S' of points x_{ij} on M' constitute a set of points obtainable one from another by a group of one-to-one reciprocal correspondences. We may consider these one-to-one correspondences as elements of a group H of operations permuting the points of S'. Among the permutations of H, will be those carrying a given point, e. g., x_{11}, regarded as initial, into other points of the same set $\{x_1\}$. The permutations leaving $\{x_1\}$ invariant form as we have seen a group G' of μ operations. When we take into consideration the manifold M, we see that the group G' leaves invariant the point x_1 on M although causing permutations among the other points. If the entire system S on M is to be generated by a single correspondence irreducible in y, we must have on M' a permutation s which carries x_{11} into some point x_{ij}, and which when multiplied by the operations of G' carries x_1, regarded as a given point x, into each of the points, y, obtained by the correspondence, $C(x, y)$. The permutation s together with the operations of G', will suffice to generate the entire system S' on M' and its image S on M. Thus H may be generated by means of the subgroup of operations $\{t\}$ of G', together with a single additional operation s not of G'. We shall say that H is generated irreducibly by s with respect to G'. If for every operation u of H and for every t_1 of G' there were another operation t_2 of G', such that $ut_1 = t_2u$, that is, if G' be a self-conjugate subgroup of H, then the same point of M would be determined no matter from what sheet of M' we started and the construction for M' would make this manifold a duplicate of M. Hence G' is not a self-conjugate subgroup of H.

It sometimes happens that the system S corresponds to a set of one-to-one transformations on M and that G' is a set of outer isomorphisms* carrying S into itself and carrying the operation s into a complete set of generators. This, although an important case is not the only one as is seen even in the simple instance of the Poncelet polygons, unless we regard the group from an abstract and non-algebraic point of view by introducing such notions as sense.

For any group H, irreducibly generated with respect to a non-self-conjugate subgroup G', we may construct a manifold M', and a manifold M with a closed correspondence system. The fundamental region of M', by means of duplicates of which M' may be constructed as a whole, is to a very large extent arbitrary,† and this degree of arbitrary choice remains, of course, in the manifold M, on which the correspondence is determined. Almost the entire theory of abstract groups and the additional theory

* Cf. Burnside, Theory of Groups, 2d ed., p. 84.

† Cf. A. Hurwitz, l. c.

incident to the particular representation of a group as irreducibly generated, as well as the theory relating to the nature of the fundamental region is reflected in the study of closed correspondences. We shall next turn to a particularly important application of the theory of closed correspondences.

Variable Inscribed Plane Configurations.

7. A system of distinct points $\{P\}$, and lines $\{l\}$, such that on each point P there lie b of the lines $\{l\}$, and on each line l, there lie a of the points $\{P\}$, where a and b are fixed finite numbers, and independent of the particular points and lines selected, will be called a *configuration*.* A configuration is *finite* whenever the total number of points and lines is finite. Any non-finite configuration must, of course, present singularities when viewed externally, and for this reason only finite configurations are usually considered. The case in which a Poncelet polygon does not close, but becomes an infinite broken line affords a simple illustration of a configuration that is not finite. Any two configurations which are in one-to-one correspondence so far as incidence relations among the given elements are concerned will be regarded as equivalent, irrespective of additional projective properties of the separate configurations. Configurations as here defined may be referred to as plane configurations in distinction from the figures in higher dimensional spaces obtained by an obvious generalization of the above definition.

Let us be given a particular configuration in the projective plane. It is clearly possible to pass an irreducible curve through all of the points of the configuration, and this, too, in an infinite number of ways, provided only that the degree of the desired curve be not previously restricted. The configuration may be said to be *inscribed* in any such curve. It sometimes happens that the curve may be so chosen in a fixed position that a certain number r, > 0, of points may be selected arbitrarily on the curve and an entire configuration equivalent to the one initially given may be constructed having the r points as points of the configuration and also, like the given one, being inscribed in the curve. The configuration may then be regarded as *varying on the curve with r degrees of freedom.*

Inscribed configurations of more than one degree of freedom present certain special problems of interest, with which, however, we shall not be concerned at this time. From the point of view of the configuration itself, the number of degrees of freedom is of relatively little significance. When there is more than one degree of freedom, we may always introduce algebraic restrictions so as to cut down the degrees of freedom to one, and it is this case, exclusively, that we shall consider.

* Cf. article in Encyc. des Sc. Math., E. Steinitz and E. Merlin, III, 9.

The Index of a Configuration, Total and Partial Configurations.

8. Let us be given an irreducible curve M, and a variable configuration K, inscribed in it, and having by virtue, perhaps, of additional conditions, one and but one degree of freedom. Let P be a point of K, and P_0 and K_0 be particular positions of P and K for which K_0 contains P_0. As P varies over M from P_0, K varies from K_0. If every possible circuit of P starting from and returning to P_0 carries the configuration K as a whole into the position K_0, then K is said to be of *total index, one.* If, however, there be τ different positions, $K_{0(1)} \equiv K_0$, $K_{0(2)}$, $\cdots$, $K_{0(\tau)}$, into which K can be carried when P returns to P_0, then the configuration is said to be of total index τ. Since the positions of the various points of the configuration are determined algebraically from the position of one variable point, P, when the position P_0 has been chosen, the remaining choices contain no free parameter and are obtainable algebraically, so that for a representative choice of P_0, τ is a finite positive integer. We shall confine ourselves to variable configurations of index one. It is readily seen that a configuration of index greater than one, generates a finite or infinite configuration of index one.

If we be given a variable, plane, inscribed configuration K, on a curve M, of one degree of freedom, and of total index one, then every point of the configuration is on one of the lines of the configuration and is a point of M, but a converse, that every point of intersection with M, by a line of the configuration, is a point of the configuration, does not follow. We shall usually be obliged to distinguish certain points not of the configuration, but on M and also on one or more of the lines of the configuration, which are fixed as the configuration varies. These will be called fixed points or base points of the configuration system. There may or may not be additional points of M on lines of the configuration, which, however, are not points of the configuration. These may be called, when existent, *extraneous variable points* of the system. When no extraneous variable points exist we shall have what we shall call a *total configuration*, otherwise, a *partial configuration.*

Configurations and Correspondences.

9. A variable configuration K, on a curve obviously establishes a closed correspondence system S on the curve, of a specially simple sort. When the configuration is of total index, one, the closed correspondence is an involution, also of index, one. The correspondence will be irreducibly generated when the following conditions are satisfied: First, if for any point P of the configuration, and a suitably chosen point P_1 on a line of the configuration containing P, we may, by a suitable circuit

on M, carry P back to its initial position and the line PP_1 into every other line of the configuration containing P. Secondly, if the correspondence from P to P_1, when repeated sufficiently often, will carry P into every one of the points of the configuration on the line PP_1. We therefore have the theorem that any irreducibly generated, variable, inscribed configuration with one degree of freedom on a curve of genus greater than one is necessarily finite.

The question arises as to whether every closed correspondence S may be interpreted as a configuration K. For various reasons the partial* configurations do not have the same interest as the total configurations. It is these latter that we shall consider.

We notice, first, that if we be given a total configuration K, the lines of K are a subset of the total number of lines of the plane, and the set of points of K, on a line of K, may be regarded as a special case of the points of intersection of an arbitrary line of the plane with the curve. As the configuration varies on the curve we shall, in any case, have a one-parameter family of lines which is a subset of the total two-parameter family, this subset being determined algebraically. Now let L be the set of points obtained by the given correspondence C, as the images on M of the set generated on M' by s alone. If C be such that L varies within a two-parameter linear family of the same order as L, and varies in such a way that no two distinct sets L of the two-parameter family contain on M as many as two common points, then we may so represent M as a curve, that S becomes the system of points in a total inscribed variable configuration K. For, by the usual theory of birational transformations, we may represent the sets L as cut out by straight lines, by means of a birational transformation, since no two distinct sets L have more than a point in common.† The set of lines in the system S are determined algebraically, giving us a line equation for a locus whose tangents determine the correspondence. The conditions that no two L-sets have more than one point of M in common and that they vary in a two-parameter linear family of the same order as L, are thus both necessary and sufficient that we have S representable as a total, variable, inscribed configuration K with one degree of freedom.

PRINCETON, N. J.,
May, 1916.

* The partial configurations are related to irrational involutions, and the total, to rational involutions.

† Severi, Lezioni, p. 18.

THE INTERSECTIONS OF A STRAIGHT LINE AND HYPERQUADRIC.

By J. L. Coolidge.

In analytic geometry of a fairly elementary sort, we frequently encounter the problem of solving simultaneously a number of linear equations, and a single quadratic equation. In homogeneous form this amounts to solving $n - 1$ linear equations, and one irreducible quadratic in $n + 1$ homogeneous variables, or, to use the jargon of projective geometry, of finding the intersections of a straight line and a hyperquadric in a space of n dimensions.

We all know that the problem can be solved, generally we content ourselves with saying that it is easy, or with writing down the single irrationality that enters into the solution. There do arise cases, however, when we must actually put the work through. We must actually have the coördinates of the intersections of a straight line and a conic, or those of the limiting points of a set of coaxal spheres, or those of the lines that intersect four skew lines in our space. The work of putting through the solution is somewhat repellant, yet when we search in the textbooks we fail to find there any solution in symmetrical form. Such, at least, has been the present writer's experience.* The fact is that every solution must be either unsymmetrical or involve arbitrary quantities dragged in from the outside. Of the two alternatives the latter is certainly preferable, and in the present paper a solution is given which seems to be about as compact and symmetrical as the problem will allow. The final form will be found in formulæ (14) and (15).

Let a point in n space have $n + 1$ homogeneous coördinates

$$x_0 : x_1 : x_2 : \cdots x_n.$$

We suppose that we have $n - 1$ homogeneous linear equations

$$(1) \qquad \sum_{i=0}^{i=n} u_i^{(1)} x_i = \sum_{i=0}^{i=n} u_i^{(2)} x_i = \cdots = \sum_{i=0}^{i=n} u_i^{(n-1)} x_i = 0$$

and a single quadratic equation

* A criterion for the reality of the solutions, when the discriminant of the quadric is not 0, is given by Snyder, "Conditions that a line," etc., Bulletin American Math. Soc., vol. 4, 1897, p. 72.

$$\sum_{i,j=0}^{i,j=n} a_{ij}x_ix_j = 0, \qquad a_{ij} = a_{ji}. \tag{2}$$

Since, by hypothesis, this quadratic form is unfactorable, the rank of the matrix $|| a_{ij} ||$ is 3 or greater. We seek for the solutions of the equations (1) and (2). We begin with the explanation of certain notations, and the development of usefu.. identities. Let

$$\Delta = \begin{vmatrix} v_0 & v_1 & \cdots & v_n \\ w_0 & w_1 & \cdots & w_n \\ u_0^{(1)} & u_1^{(1)} & \cdots & u_n^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ u_0^{(n-1)} & u_1^{(n-1)} & \cdots & u_{(n)}^{(n-1)} \end{vmatrix}, \tag{3}$$

$$p_{ij} = -p_{ji} = \frac{1}{\Delta}\left(\frac{\partial\Delta}{\partial v_i}\frac{\partial\Delta}{\partial w_j} - \frac{\partial\Delta}{\partial v_j}\frac{\partial\Delta}{\partial w_i}\right). \tag{4}$$

The quantities p_{ij} are independent of v and w; they are the Plücker coördinates of the line in question. They are connected by certain interesting identities

$$2(p_{ij}p_{kl} + p_{ik}p_{lj} + p_{il}p_{jk}) = \frac{1}{\Delta^2}\begin{vmatrix} \frac{\partial\Delta}{\partial v_i} & \frac{\partial\Delta}{\partial v_j} & \frac{\partial\Delta}{\partial v_k} & \frac{\partial\Delta}{\partial v_l} \\ \frac{\partial\Delta}{\partial w_i} & \frac{\partial\Delta}{\partial w_j} & \frac{\partial\Delta}{\partial w_k} & \frac{\partial\Delta}{\partial w_l} \\ \frac{\partial\Delta}{\partial v_i} & \frac{\partial\Delta}{\partial v_j} & \frac{\partial\Delta}{\partial v_k} & \frac{\partial\Delta}{\partial v_l} \\ \frac{\partial\Delta}{\partial w_i} & \frac{\partial\Delta}{\partial w_j} & \frac{\partial\Delta}{\partial w_k} & \frac{\partial\Delta}{\partial w_l} \end{vmatrix} = 0, \tag{5}$$

$$\begin{vmatrix} 0 & p_{ij} & p_{ik} & p_{il} \\ p_{ji} & 0 & p_{jk} & p_{jl} \\ p_{ki} & p_{kj} & 0 & p_{kl} \\ p_{li} & p_{lj} & p_{lk} & 0 \end{vmatrix} = 0, \tag{6}$$

$$\begin{vmatrix} p_{ij} & p_{ik} & p_{il} \\ 0 & p_{jk} & p_{jl} \\ p_{kj} & 0 & p_{kl} \end{vmatrix} = 0. \tag{7}$$

Consider next the determinant

$$(8) \qquad \begin{vmatrix} 0 & p_{ij} & p_{ik} & \cdots & p_{iy} \\ p_{ji} & 0 & p_{jk} & \cdots & p_{jy} \\ p_{ki} & p_{kj} & 0 & \cdots & p_{ky} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{yi} & p_{yj} & p_{yk} & \cdots & 0 \end{vmatrix}.$$

This is skew symmetric, and hence vanishes when its order is odd. It is also equal to zero when the order is four, as we see by (6). In general, when the order is even it is the perfect square of a function that is linear in a system of like determinants of an order two less,* and so vanishes if its order is even and greater than four. In other words, this determinant vanishes in every case when the order is other than 2. Likewise, consider

$$(9) \qquad \begin{vmatrix} p_{ij} & p_{ik} & \cdots & p_{iy} & p_{iz} \\ 0 & p_{jk} & \cdots & p_{jy} & p_{jz} \\ p_{kj} & 0 & \cdots & p_{ky} & p_{kz} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{yj} & p_{yk} & \cdots & 0 & p_{yz} \end{vmatrix}.$$

If we expand in terms of the elements of the last column, each cofactor is either of the present form and lower order, or of the form (8). The latter can be at once rejected, and the former gradually whittled down to (7). Hence (9) vanishes when its degree is above 2. The last two results can be combined in a single identity

$$(10) \qquad \begin{vmatrix} z_0 & p_{ij} & p_{ik} & \cdots & p_{iy} \\ z_1 & 0 & p_{jk} & \cdots & p_{jy} \\ z_2 & p_{kj} & 0 & \cdots & p_{ky} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ z_r & p_{yj} & p_{yk} & \cdots & 0 \end{vmatrix} \equiv 0, \qquad r > 2.$$

We have now, fortunately, finished our preliminary work, and may proceed at once to the problem in hand. Let us suppose, as a first case, that equations (1) and (2) have been so far modified by a collineation of space, that the latter reduces to the form

$$\sum_{i=0}^{i=n} a_i x_i^2 \equiv \sum_{i=0}^{i=n} (a_i x_i) x_i = 0.$$

This latter form appears as quasi-linear in (x). Adding this to the linear

* Conf. Kowalewski, "Determinantentheorie," Leipzig, 1909, pp. 134 ff.

equations (1) we have n linear equations in $n+1$ homogeneous variables. Solving these in the usual way we find

$$(11) \qquad -px_k = \frac{\partial}{\partial t_k}\begin{vmatrix} t_0 & t_1 & \cdots & t_n \\ u_0^{(1)} & u_1^{(1)} & \cdots & u_n^{(1)} \\ \cdot & \cdot & \cdots & \cdot \\ u_0^{(n-1)} & u_1^{(n-1)} & \cdots & u_n^{(n-1)} \\ a_0x_0 & a_1x_1 & \cdots & a_nx_n \end{vmatrix}.$$

This time we have $n+1$ really linear equations in as many variables, the condition of compatibility gives the following equation in p

$$\begin{vmatrix} p & a_1p_{01} & a_2p_{02} & \cdots & a_np_{0n} \\ a_0p_{10} & p & a_2p_{12} & \cdots & a_np_{1n} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ a_0p_{n0} & a_1p_{n1} & a_2p_{n2} & \cdots & p \end{vmatrix} = 0.$$

The coefficient of each power of p below the three highest is of the form (8) and so is equal to zero. We have, thus,

$$(12) \qquad p^2 + \tfrac{1}{2}\sum_{i,j=0}^{i,j=n} a_ia_jp_{ij}^2 = 0.$$

If we take p from this equation, our equations (11) are consistent. We might omit any one of them, and find the ratios of our variables from the remainder. Such a set of solutions would, however, be unsymmetrical, owing precisely to the rejection of one equation. It is preferable to multiply through the solutions obtained by rejecting the ith equation by an arbitrary multiplier z_i and take the sum. We thus get x_0, for instance

$$\rho x_0 = \begin{vmatrix} z_0 & a_1p_{01} & a_2p_{02} & \cdots & a_np_{0n} \\ z_1 & p & a_2p_{12} & \cdots & a_np_{1n} \\ z_2 & a_1p_{21} & p & \cdots & a_np_{2n} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ z_n & a_1p_{n1} & a_2p_{n2} & \cdots & p \end{vmatrix}.$$

Expanding in terms of p, we see, by (10) that the coefficients of all but the three highest powers of p are zero. Dividing through by p^{n-2}

$$\rho x_0 = z_0p^2 - p\sum_{i=0}^{i=n} a_iz_ip_{0i} + \tfrac{1}{2}\sum_{i,j=0}^{i,j=n} a_ia_jp_{ij}(z_0p_{ij} + z_ip_{j0} + z_jp_{0i}).$$

Remembering (12) and putting

$$P_{ki} = \sum_{j=0}^{j=n} a_j p_{kj} p_{ji},$$

$$\rho x_k = \sum_{i=0}^{i=n} a_i z_i (P_{ki} - p p_{ki}). \tag{13}$$

It only remains to rewrite this in invariant form when the hyperquadric has the general equation (2). We write first

$$p^2 + \frac{1}{2} \sum_{l,\, i=0}^{l,\, i=n} \sum_{m,\, j=0}^{m,\, j=n} a_{li} a_{mj} p_{lm} p_{ij} = 0. \tag{14}$$

Then, by frequent use of (5) we find

$$\rho x_k = \sum_{l,\, i=0}^{l,\, i=n} \left[a_{li} z_i \left(\sum_{m,\, j=0}^{m,\, j=n} a_{mj} p_{lm} p_{kj} + p p_{lk} \right) \right]. \tag{15}$$

CAMBRIDGE, MASS.,
December, 1916.

THE RELATION BETWEEN THE ZEROS OF A SOLUTION OF A LINEAR HOMOGENEOUS DIFFERENTIAL EQUATION AND THOSE OF ITS DERIVATIVES.

By William Benjamin Fite.

The fact that a non-identically vanishing solution of a linear homogeneous differential equation of order n and its first $n - 1$ derivatives cannot all vanish at a point* raises the question as to the existence of a length so small that no solution and its first $n - 1$ derivatives can all vanish within an interval of this length. In the first part of this paper I show that this question must be answered in the affirmative. This is done by determining such a length for any given equation. In the second part I consider in some detail such lengths in connection with equations of the second order. I also show that in certain cases there must be a root of the derivative of a solution of such an equation within a given distance from a root of the solution.

I.

Consider, for the sake of definiteness, the linear homogeneous differential equation of the third order

$$y''' + py'' + qy' + ry = 0, \tag{1}$$

and suppose that y is any non-identically vanishing solution such that y, y', and y'' all vanish within the interval (a, b) $(b > a)$.

If P, Q, and R are constants such that $|p| \leqq P$, $|q| \leqq Q$, and $|r| \leqq R$ within (a, b), and if M_y, $M_{y'}$, $M_{y''}$ and $M_{y'''}$ are the greatest absolute values of y, y', y'', and y''' respectively in the interval, then

$$M_y \leqq lM_{y'}, \qquad M_{y'} \leqq lM_{y''}, \qquad M_{y''} \leqq lM_{y'''},$$

where $b - a = l$. Moreover

$$M_{y'''} \leqq PM_{y''} + QM_{y'} + RM_y.$$

Hence

$$M_{y'''} \leqq PlM_{y'''} + Ql^2M_{y'''} + Rl^3M_{y'''},$$

or†

* It will be assumed throughout this paper that the coefficients of y and its derivatives in the equations discussed are continuous functions of x within certain intervals.

† If $M_{y'''} = 0$, y, y', and y'' cannot all vanish in the interval (a, b).

$$Rl^3 + Ql^2 + Pl - 1 \geqq 0.$$

Now the equation

$$Rl^3 + Ql^2 + Pl - 1 = 0 \tag{2}$$

has just one positive root, say l_1; and therefore we must have $l \geqq l_1$. But if it were possible to have $l = l_1$, we should have to have $M_y = lM_{y'}$. This would require y' to be a constant, and therefore zero, since by hypothesis it is zero at one point of (a, b). Then y would be identically zero. Hence any interval within which y, y', and y'' all vanish must be greater in length than the positive root of equation (2) in which P, Q, and R are taken with reference to some fundamental interval within which we are operating.

This reasoning is applicable to any equation of order n $(n > 1)$ and leads to the conclusion that any interval within which any non-identically vanishing solution of a linear homogeneous differential equation of order n, together with its first $n - 1$ derivatives, vanishes must be greater in length than the positive root of an equation analogous to (2).

If we are dealing with complex quantities a similar argument shows that a non-identically vanishing solution and its first $n - 1$ derivatives cannot all vanish within a circle of diameter l which lies within a region within which the coefficients are all analytic unless l exceeds the positive root of an equation analogous to (2).

II.

Consider now the equation of the second order

$$y'' + py' + qy = 0. \tag{3}$$

If $q \leqq 0$ throughout an interval (a, b), there is no non-identically vanishing solution y of (3) such that $y(a) = 0$ or $y(b) = 0$, and $y'(c) = 0$, when $a \leqq c \leqq b$.* Moreover, if $q < 0$ and y does not vanish in (a, b), y'/y cannot change from positive to zero or from zero to negative.

A solution y_1 of the equation

$$y'' + p_1y' + q_1y = 0, \tag{4}$$

where $p_1 \geqq p$, $q_1 \geqq q$, and $q_1 > 0$ in (a, b), such that $y_1'(c) = 0$ $(a < c \leqq b)$, must vanish for some value of x in the interval (a, c), provided that there is a solution y of (3) such that $y(a) = 0$ and $y'(c) = 0$. For if this were not the case we could assume that $y_1(x) > 0$ in this interval (including c), and then the function $\bar{y}$ defined by the relation $y = y_1\bar{y}$ would be a solution of the equation

* Bôcher, Transactions of the American Mathematical Society, vol. 3 (1902), p. 199, theorem IV.

$$\bar{y}'' + \frac{2y_1' + py_1}{y_1}\bar{y}' + \frac{y_1'' + py_1' + qy_1}{y_1}\bar{y} = 0 \qquad (5)$$

such that $\bar{y}(a) = 0$ and $\bar{y}'(c) = 0$. Now by hypothesis $y_1'(c) = 0$ and therefore $y_1''(c) < 0$ since $q_1 > 0$. It follows from this that $y_1' > 0$ for values of x a little less than c. If y_1' were negative for any value of x in (a, c), there would be at least one value of x $(\neq c)$ in this interval for which $y_1' = 0$ and $y_1'' < 0$. But if d were the greatest such value, y_1' could not be positive in (d, c). We conclude therefore that $y_1' \geqq 0$, and hence that $y_1'' + py_1' + qy_1 \leqq 0$, in (a, c). This is however impossible since $\bar{y}(a) = 0$ and $\bar{y}'(c) = 0$. This establishes the statement that $y_1(x)$ vanishes in the interval (a, c).

If there were a solution y_2 of (4) such that $y_2(a) = 0$ and $y_2'(x) > 0$ in the closed interval (a, c), we should have

$$y_1(c + h) - y_2(c + h) = y_1(c) - y_2(c) + [y_1'(c + \theta h) - y_2'(c + \theta h)]h \qquad (0 < \theta < 1).$$

If we so select y_1 and y_2 that $y_1(c) = y_2(c)$, it follows that $y_1(c + h) - y_2(c + h) > 0$ for small negative values of h. Moreover there would be in the interval a value of x for which $y_1(x) - y_2(x) < 0$; namely, a value of x for which $y_1(x) = 0$. Hence these two solutions would have at least two points in common in (a, c). This being obviously impossible, we have the following important theorem of comparison for the solutions of equations (3) and (4):

THEOREM I. *If y and y_1 are non-identically vanishing solutions of equations* (3) *and* (4) *respectively such that $y(a) = y_1(a) = 0$ and $y'(c) = 0$, then $y_1'(x)$ vanishes somewhere in the interval (a, c).*

If we substitute the equation

$$y'' + p_2y' + q_1y = 0, \qquad (6)$$

where $p_2 \leqq p$ in (a, b), for equation (4), a slight and obvious modification of the foregoing reasoning establishes

THEOREM II. *If y and y_1 are non-identically vanishing solutions of equations* (3) *and* (6) *respectively such that $y(b) = y_1(b) = 0$ and $y'(c) = 0$, then $y_1'(x)$ vanishes somewhere in the interval (c, b).*

If we take for the functions p_1 and q_1 constants M and H respectively, equation (4) becomes

$$y'' + My' + Hy = 0. \qquad (7)$$

These constants can always be so selected that $M^2 - 4H < 0$. When this has been done, the solution of (7) that vanishes for $x = a$ is of the form

$$y_1(x) = Ae^{-Mx/2}\left(\sin\frac{\sqrt{4H - M^2}}{2}x - \tan\frac{\sqrt{4H - M^2}}{2}a \cdot \cos\frac{\sqrt{4H - M^2}}{2}x\right).$$

The roots d of the equation $y_1'(x) = 0$ are given by the formula

$$d - a = \frac{2 \text{ arc tg}\dfrac{\sqrt{4H - M^2}}{M}}{\sqrt{4H - M^2}}.$$

We have proved therefore

THEOREM III. *If a non-identically vanishing solution y of equation (3) is such that $y(a) = 0$, its derivative cannot vanish for $x = c$ $(c > a)$ when $4H - M^2 > 0$, unless*

$$c - a \geqq \frac{2 \text{ arc tg}\dfrac{\sqrt{4H - M^2}}{M}}{\sqrt{4H - M^2}},$$

where

$$\text{arc tg}\frac{\sqrt{4H - M^2}}{M}$$

has its least positive value.

If $y(b) = 0$, its derivative cannot vanish for $x = c$ $(c < b)$ unless

$$b - c \geqq \left|\frac{2 \text{ arc tg}\dfrac{\sqrt{4H - m^2}}{m}}{\sqrt{4H - m^2}}\right|,$$

where M is less than or equal to p in the interval considered and its least negative value is to be given to the arc tangent.

For example, consider the solutions of Bessel's equation,

$$y'' + \frac{1}{x}y' + \left(1 - \frac{n^2}{x^2}\right)y = 0.$$

We can take $M = 1/a$ and $H = 1$. Then

$$\lim_{a\to\infty}\frac{2 \text{ arc tg}\dfrac{\sqrt{4H - M^2}}{M}}{\sqrt{4H - M^2}} = \frac{\pi}{2}.$$

Hence, if ϵ is an arbitrarily chosen positive number, we can choose m so large that if y is any solution of this equation such that $y(a) = 0$ and $a > m$ then $y'(c) \neq 0$ $(c > a)$ unless $c - a > (\pi/2) - \epsilon$. A similar conclusion holds for $b - c$ $(c < b)$ in case $y(b) = 0$.

If $M^2 - 4H = 0$ the solution of (7) that vanishes for $x = a$ is

$$y_1(x) = Ae^{-Mx/2}(x - a).$$

If $y_1'(c) = 0$ then $c - a = 2/M$. Hence, if $M < 0$, y_1' does not vanish for any value of x greater than a, and therefore under these circumstances, if y vanishes for $x = a$, y' does not vanish for any value of x greater than a.

In case $y(a) \neq 0$ consider the inequality

$$c - a < \frac{4y'(a)}{M^2y(a) + 2My'(a)}. \tag{8}$$

If M, $y(a)$, and $y'(a)$ are all positive, (8) carries with it the inequalities

$$\frac{y'(a)}{y(a)} > \frac{M}{2 - (c - a)M} - \frac{M}{2} \tag{9}$$

and

$$c - a < \frac{2}{M}.$$

Hence when (8) holds equation (7) has a solution y_1 such that $y_1(x) > 0$ for $a \leqq x \leqq c$ and $y_1'(c) = 0$. This solution is

$$y_1(x) = Ae^{-Mx/2}[2 - (c - x)M].$$

But when we use this y_1 in (5) we have $[\bar{y}'(a)]/[\bar{y}(a)] > 0$, as a consequence of (9). This however would be impossible if $y'(c) = 0$. The preceding discussion shows that (8) and $y'(c) = 0$ are inconsistent also when $y(a) = 0$. Moreover, since M and H are restricted only from below, we can always so select them that $M^2 - 4H = 0$.

If m satisfies the inequalities $m < 0$ and $m \leqq p$ in (a, b), we can apply a similar argument to (c, b). Hence

THEOREM IV. *If y is any non-identically vanishing solution of equation (3) such that either $y(a) = 0$ or $[y'(a)]/[y(a)] > 0$, then $y'(c) \neq 0$ when $a < c \leqq b$ and $c - a < [4y'(a)]/[M^2y(a) + 2My'(a)]$, where M satisfies the inequalities $M > 0$, $M \geqq p$, and $M^2 \geqq 4q$, in (a, b).**

If either $y(b) = 0$ or $[y'(b)]/[y(b)] < 0$, then $y'(c) \neq 0$ when $a \leqq c < b$ and $b - c < [-4y'(b)]/[m^2y(b) + 2my'(b)]$, where m satisfies the inequalities $m < 0$, $m \leqq p$, and $m^2 \geqq 4q$, in (a, b).

If in equation (3) we have $q > 0$ we can readily determine intervals within which some solution of this equation and its derivative both vanish. Consider the equation

$$y'' + my' + hy = 0, \tag{10}$$

where m and h are constants such that $m \leqq p$ and $h \leqq q$ within (a, b). If $m^2 - 4h < 0$ and y_1 is a solution of (10) such that $y_1(a) = 0$, then $y_1'(c) = 0$, in case

* The case $M^2 - 4H > 0$ might also be discussed, but I pass over it since it can be brought under the other cases.

$$c - a = \frac{2 \text{ arc tg} \dfrac{\sqrt{4h - m^2}}{m}}{\sqrt{4h - m^2}},$$

where its least positive value is to be given to arc tg $[\sqrt{4h - m^2}]/m$. It follows from Theorem I that if y is a solution of (3) such that $y(a) = 0$. then y' must vanish in the interval

$$\left(a,\ a + \frac{2 \text{ arc tg} \dfrac{\sqrt{4h - m^2}}{m}}{\sqrt{4h - m^2}}\right).$$

Similarly if $m^2 - 4h = 0$ and $y(a) = 0$, then y' must vanish in the interval

$$\left(a,\ a + \frac{2}{m}\right),$$

in case $m > 0$.

If $m^2 - 4h > 0$ and y_1 is a solution of (10) such that $y_1(a) = 0$, then $y_1'(c) = 0$, where

$$c - a = \frac{\log \dfrac{-m - \sqrt{m^2 - 4h}}{-m + \sqrt{m^2 - 4h}}}{\sqrt{m^2 - 4h}}.$$

This expression for $c - a$ is positive when $m > 0$ and $h > 0$. Hence under these conditions if $y(a) = 0$, y' must vanish in the interval (a, c). Analogous conditions can readily be obtained under which y' must vanish within a certain interval (c, b) $(c < b)$ in case $y(b) = 0$.

If y is a non-identically vanishing solution of (3) and if $q > 0$ for $a \leqq x \leqq b$, y' cannot vanish more than once between two consecutive roots of y in this interval. Moreover it must vanish at least once. If then a and b are two consecutive roots of y and if $y(x) > 0$ for $a < x < b$, let c be the root of y' in this interval. If we suppose that $p > 0$ throughout the closed interval, y'' cannot vanish for either $x = a$ or $x = c$, since otherwise we should have either $y'(a) = 0$ or $y(c) = 0$. If $y''(x)$ vanishes for $a < x < c$, we should have $y'(x) < 0$ for this value of x. But this is impossible since $y'(a) > 0$ and $y'(x) \neq 0$ for any value of x between a and c. On the other hand, $y''(c) < 0$ and $y''(b) > 0$ since $y'(b) < 0$ and $y(b) = 0$. Hence $y''(x)$ has at least one root between c and b.

If $p < 0$ throughout (a, b) and the other conditions remain unchanged, y'' has at least one root in (a, c) and none at all in (c, b).

If now p and q possess continuous derivatives throughout (a, b) we can differentiate the left number of (3) and in the result substitute for y its value as given by (3). This gives

$$y''' + \left(p - \frac{q'}{q}\right)y'' + \left(p' + q - \frac{pq'}{q}\right)y' = 0. \tag{9}$$

Now

$$p' + q - \frac{pq'}{q} = q\left[\frac{d}{dx}\left(\frac{p}{q}\right) + 1\right].$$

Hence $p' + q - (pq'/q)$ and $(d/dx)(p/q) + 1$ have the same sign, since by hypothesis $q > 0$. It follows that if $(d/dx)(p/q) \leqq -1$ in (a, b) then y' and y'' cannot both vanish in this interval. We have therefore

THEOREM V. *If $q > 0$ and $(d/dx)(p/q) \leqq -1$ in (a, b), no root of y can follow a root of y' in case $p > 0$, and no root of y' can follow a root of y in case $p < 0$.*

CONJUGATE PLANAR NETS WITH EQUAL INVARIANTS.

By Luther Pfahler Eisenhart.

Koenigs* has shown by geometrical considerations that the perspectives of the asymptotic lines on a surface from a point on a plane form a conjugate net with equal invariants; that is, the homogeneous coördinates y_1, y_2, y_3, of the plane, expressed in terms of parameters u and v referring to the planar net, are solutions of a system of equations of the form

$$\begin{aligned} y_{uu} &= ay_u + by_v + cy, \\ y_{uv} &= (\log \sigma)_v y_u + (\log \sigma)_u y_v + c'y, \\ y_{vv} &= a''y_u + b''y_v + c''y, \end{aligned} \tag{1}$$

where in general the coefficients are functions of u and v. Koenigs observed, conversely, that such a planar net may be regarded as the perspective of the asymptotic lines on a surface. He stated that the surface can be found by quadratures, but did not give a proof. It is the purpose of this note to establish this converse theorem, at the same time giving the quadratures involved in the determination of the surface. It is an interesting fact that the formulas of Lelieuvre arise as a special case of the problem.

In order that equations (1) shall be completely integrable, and thus admit three linearly independent solutions, the coefficients must satisfy six conditions obtained from the integrability requirements

$$(y_{uu})_v = (y_{uv})_u, \qquad (y_{uv})_v = (y_{vv})_u.$$

We shall not write down these conditions, but merely remark that one of them is $a_v = b_u$, which may be replaced by

$$a = \frac{\partial \log \rho}{\partial u}, \qquad b = \frac{\partial \log \rho}{\partial v}, \tag{2}$$

where ρ is thus defined.

It is well known† that when the first and third of equations (1) admit four linearly independent solutions, they are the homogeneous point coördinates of a surface upon which the parametric curves are the asymp-

* Comptes Rendus, vol. 114 (1892), p. 55. Recently an analytic proof has been given by A. L. Nelson, Rendiconti di Palermo, vol. 42 (1916).

† Darboux, Leçons, second edition, vol. 1, p. 205.

$$y''' + \left(p - \frac{q'}{q}\right)y'' + \left(p' + q - \frac{pq'}{q}\right)y' = 0. \tag{9}$$

Now

$$p' + q - \frac{pq'}{q} = q\left[\frac{d}{dx}\left(\frac{p}{q}\right) + 1\right].$$

Hence $p' + q - (pq'/q)$ and $(d/dx)(p/q) + 1$ have the same sign, since by hypothesis $q > 0$. It follows that if $(d/dx)(p/q) \leqq -1$ in (a, b) then y' and y'' cannot both vanish in this interval. We have therefore

THEOREM V. *If $q > 0$ and $(d/dx)(p/q) \leqq -1$ in (a, b), no root of y can follow a root of y' in case $p > 0$, and no root of y' can follow a root of y in case $p < 0$.*

CONJUGATE PLANAR NETS WITH EQUAL INVARIANTS.

By Luther Pfahler Eisenhart.

Koenigs* has shown by geometrical considerations that the perspectives of the asymptotic lines on a surface from a point on a plane form a conjugate net with equal invariants; that is, the homogeneous coördinates y_1, y_2, y_3, of the plane, expressed in terms of parameters u and v referring to the planar net, are solutions of a system of equations of the form

$$\begin{aligned} y_{uu} &= ay_u + by_v + cy, \\ y_{uv} &= (\log \sigma)_v y_u + (\log \sigma)_u y_v + c'y, \\ y_{vv} &= a''y_u + b''y_v + c''y, \end{aligned} \tag{1}$$

where in general the coefficients are functions of u and v. Koenigs observed, conversely, that such a planar net may be regarded as the perspective of the asymptotic lines on a surface. He stated that the surface can be found by quadratures, but did not give a proof. It is the purpose of this note to establish this converse theorem, at the same time giving the quadratures involved in the determination of the surface. It is an interesting fact that the formulas of Lelieuvre arise as a special case of the problem.

In order that equations (1) shall be completely integrable, and thus admit three linearly independent solutions, the coefficients must satisfy six conditions obtained from the integrability requirements

$$(y_{uu})_v = (y_{uv})_u, \qquad (y_{uv})_v = (y_{vv})_u.$$

We shall not write down these conditions, but merely remark that one of them is $a_v = b_u$, which may be replaced by

$$a = \frac{\partial \log \rho}{\partial u}, \qquad b = \frac{\partial \log \rho}{\partial v}, \tag{2}$$

where ρ is thus defined.

It is well known† that when the first and third of equations (1) admit four linearly independent solutions, they are the homogeneous point coördinates of a surface upon which the parametric curves are the asymp-

* Comptes Rendus, vol. 114 (1892), p. 55. Recently an analytic proof has been given by A. L. Nelson, Rendiconti di Palermo, vol. 42 (1916).

† Darboux, Leçons, second edition, vol. 1, p. 205.

totic lines. There are four conditions to be satisfied by the coefficients of two such equations in order that they shall admit four linearly independent solutions. These conditions follow from the requirement that the equation

$$(y_{uu})_{vv} = (y_{vv})_{uu}$$

shall be satisfied identically. One of them is equivalent to (2), and the other three are satisfied when the system (1) is completely integrable. Hence when the system (1) is completely integrable, there exists a solution of the first and third of equations (1) linearly independent of the three linearly independent solutions of the system. Consequently the parametric asymptotic net on the surface whose point coördinates are these four solutions, is perspective with the planar net, defined by (1), from the vertex of the tetrahedron of reference not on the plane. Hence we have established the converse of the theorem of Koenigs. But we are interested primarily in showing how the fourth solution of the first and third of equations (1) can be found by three quadratures, when three linearly independent solutions of the system (1) are known. The remainder of the paper is concerned with this problem and certain corollaries.

3. It is desirable to recall the method of reducing to a quadrature the solution of an ordinary linear differential equation of order n when $n - 1$ linearly independent solutions are known.* We take the case $n = 4$ (as this applies to the problem in hand), and write the equation

$$\frac{d^4y}{dx^4} + \alpha\frac{d^3y}{dx^3} + \beta\frac{d^2y}{dx^2} + \gamma\frac{dy}{dx} + \delta y = 0. \tag{3}$$

Let y_1, y_2, y_3 be three linearly independent solutions and write

$$y = C_1y_1 + C_2y_2 + C_3y_3, \tag{4}$$

where C_i are functions of x subject to the conditions

$$\sum_{i=1}^{3} y_i\frac{dC_i}{dx_i} = 0, \qquad \sum_{i=1}^{3} \frac{dy_i}{dx}\frac{dC_i}{dx} = 0. \tag{5}$$

When we require that y as given by (4) shall satisfy equation (3), we get

$$\sum_{i=1}^{3}\left(2\frac{dC_i}{dx}\frac{d^3y_i}{dx^3} + \frac{d^2C_i}{dx^2}\frac{d^2y_i}{dx^2} + \alpha\frac{dC_i}{dx}\frac{d^2y_i}{dx^2}\right) = 0. \tag{6}$$

In order to give this equation a suitable form, we make use of the determinant

* Forsyth, Differential Equations, third edition, pp. 128–130.

$$\Delta = \begin{vmatrix} \frac{d^2y_1}{dx^2} & \frac{d^2y_2}{dx^2} & \frac{d^2y_3}{dx^2} \\ \frac{dy_1}{dx} & \frac{dy_2}{dx} & \frac{dy_3}{dx} \\ y_1 & y_2 & y_3 \end{vmatrix}, \tag{7}$$

and indicate by Δ_i the cofactor of d^2y_i/dx^2. From (5) we get

$$\frac{\frac{dC_1}{dx}}{\Delta_1} = \frac{\frac{dC_2}{dx}}{\Delta_2} = \frac{\frac{dC_3}{dx}}{\Delta_3} = z,$$

z being thus defined. Hence we have

$$\frac{d^2C_i}{dx^2} = \Delta_i \frac{dz}{dx} + z\frac{d\Delta_i}{dx}.$$

When these values are substituted in (6), the resulting equation is reducible to the form

$$\frac{d}{dx} \log z\Delta^2 = -\alpha.$$

Consequently

$$z = \frac{A}{\Delta^2} e^{-\int a\,dx}, \qquad C_i = A\int \frac{\Delta_i}{\Delta^2} e^{-\int a\,dx}\,dx,$$

where A is an arbitrary constant. The latter can in all generality be taken equal to unity, so that the integral (4) is

$$y = \Sigma y_i \int \frac{\Delta_i}{\Delta^2} e^{-\int a\,dx}\,dx, \tag{8}$$

which evidently is linearly independent of y_1, y_2, and y_3.

4. If the first of equations (1) be differentiated twice with respect to u, the resulting equation is reducible by means of the first and third of (1) to

$$y_{uuuu} - 2(\log b\rho)_u y_{uuu} + Py_{uu} + Qy_u + Ry = 0, \tag{9}$$

where P, Q, R are determinate functions of u and v whose form is unessential to the subsequent study.

For the present we look upon equation (9) as an ordinary differential equation with v appearing as a parameter in the coefficients, and apply the method of § 3, on the supposition that we know the planar net, that is the homogeneous coördinates y_1, y_2, y_3 satisfying (1), which are three linearly independent solutions of (9). Now Δ has the form

$$\Delta = \begin{vmatrix} \frac{\partial^2 y_1}{\partial u^2} & \frac{\partial^2 y_2}{\partial u^2} & \frac{\partial y_3}{\partial u^2} \\ \frac{\partial y_1}{\partial u} & \frac{\partial y_2}{\partial u} & \frac{\partial y_3}{\partial u} \\ y_1 & y_2 & y_3 \end{vmatrix}.$$

If this equation be differentiated with respect to u, the result is reducible to

$$\frac{\partial \Delta}{\partial u} = \Delta \frac{\partial}{\partial u} \log (b\sigma\rho).$$

Hence for the present case the integral (8) becomes

$$y = \sum_{i=1}^{3} y_i \int \frac{\Delta_i}{\sigma^2} du.$$

If we had proceeded in a similar way by differentiating twice with respect to v the third of equations (1), we should have obtained the integral

$$y = \sum_{i=1}^{3} y_i \int \frac{\Delta_i'}{\sigma^2} dv,$$

where Δ_i' are the cofactors of the terms of the first row of

$$\Delta' = \begin{vmatrix} \frac{\partial^2 y_1}{\partial v^2} & \frac{\partial^2 y_2}{\partial v^2} & \frac{\partial^2 y_3}{\partial v^2} \\ \frac{\partial y_1}{\partial v} & \frac{\partial y_2}{\partial v} & \frac{\partial y_3}{\partial v} \\ y_1 & y_2 & y_3 \end{vmatrix}.$$

In order to coördinate these results, we observe that for $i = 1, 2, 3$; $j = 1, 2, 3$, but $i \neq j$,

$$\left(\frac{y_i y_{ju} - y_j y_{iu}}{\sigma^2}\right)_v + \left(\frac{y_i y_{jv} - y_j y_{iv}}{\sigma^2}\right)_u = 0.$$

Hence looking upon u and v as independent variables, we note that a fourth integral of the first and third of equations (1) is given by

$$y_4 = x_1 y_1 + x_2 y_2 + x_3 y_3, \tag{10}$$

where the functions x_i are given by the quadratures

$$x_{1u} = \frac{1}{\sigma^2}(y_2 y_{3u} - y_3 y_{2u}), \qquad x_{1v} = -\frac{1}{\sigma^2}(y_2 y_{3v} - y_3 y_{2v}), \tag{11}$$

and similar expressions obtained by permuting the subscripts cyclically.

5. Since any linear expression with constant coefficients of y_1, y_2, y_3, y_4 is likewise a solution of the first and third of equations (1), there are ∞^4 asymptotic nets which are perspective with the planar net from the vertex of the coördinate tetrahedron not in the plane of the given net.

6. From (11) we have by differentiation

$$(12)\qquad \begin{aligned} x_{iuu} &= \left(a - \frac{2\sigma_u}{\sigma}\right)x_{iu} - bx_{iv}, \\ x_{ivv} &= -a''x_{iu} + \left(b'' - \frac{2\sigma_v}{\sigma}\right)x_{iv}. \end{aligned}$$

Hence x_1, x_2, x_3, 1 are the homogeneous point coördinates of a surface X referred to its asymptotic lines.

From (10) it follows that X is the polar of the surface Y with the point coördinates y_1, y_2, y_3, y_4, with respect to the quadric

$$z_1^2 + z_2^2 + z_3^2 - z_4^2 = 0.$$

The functions y_i may also be looked upon as tangential coördinates of X. Consequently y_1, y_2, y_3 are the tangential coördinates of the planar net enveloped by the lines of intersection of the tangent planes to X and the plane $z_4 = 0$.

7. If we put

$$\nu_i = \frac{y_i}{\sigma},$$

equation (10) becomes

$$\nu_4 = x_1\nu_1 + x_2\nu_2 + x_3\nu_3,$$

and (11) may be replaced by

$$(13)\qquad x_{1u} = \nu_2\nu_{3u} - \nu_3\nu_{2u}, \qquad x_{1v} = -(\nu_2\nu_{3v} - \nu_3\nu_{2v}).$$

If now we take $z_4 = 0$ as the plane at infinity, and the other edges of the coördinate tetrahedron are mutually perpendicular, the functions ν_1, ν_2, ν_3 are proportional to the direction-cosines of the normal to X, and equations (13) are the well-known formulas of Lelieuvre.*

8. In order that the coördinates of the given planar net may be cartesian, the functions c in equations (1) must be zero. In this case we put $y_3 = 1$ in (10) and (11), so that the given net is the orthogonal projection of the asymptotic parametric net on the surface whose cartesian coördinates are y_1, y_2, y_4.

* Cf. the author's Differential Geometry, p. 193.

PRINCETON UNIVERSITY.

SEPTEMBER, 1916

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

EDITED BY

ORMOND STONE
L. P. EISENHART
OSWALD VEBLEN
PIERRE BOUTROUX
T. H. GRONWALL
J. H. M. WEDDERBURN

WITH THE COÖPERATION OF

J. W. ALEXANDER
A. A. BENNETT
H. H. MITCHELL

PUBLISHED UNDER THE AUSPICES OF PRINCETON UNIVERSITY

SECOND SERIES, VOL. 18, NO. 1

LANCASTER, PA., AND PRINCETON, N. J.

CONTENTS

PAGE

On the Surface of Lowest Degree Passing through a Given Curve in Space. By T. HAYASHI 1

A Practical Method of Determining Elementary Divisors. By H. T. BURGESS 4

Conjugate Systems with Equal Point Invariants. By L. P. EISENHART 7

On the Derivatives of a Function at a Point. By J. F. RITT . . . 18

An Existence Theorem for the Solution of a Type of Real Mixed Difference Equation. By A. A. BENNETT 24

Double Elliptic Geometry in Terms of Point and Order Alone. By J. R. KLINE 31

An Application of a Group of Order 16 to a Configuration of an Elliptic Cubic. By A. EMICH 45

Copies of the following memoir can be obtained by addressing THE ANNALS OF MATHEMATICS, Princeton, N. J.:

An Elementary Exposition of the Theory of the Gamma Function. By J. L. W. V. JENSEN. Authorized translation with additional notes by T. H. GRONWALL. 43 pages. Price 50 cents.

ANNALS OF MATHEMATICS

Published in September, December, March and June, at Lancaster, Pa. and Princeton, N. J., U. S. A.

Communications should be addressed to The Editors of the *Annals of Mathematics*, Princeton, N. J., U. S. A. Subscription price, $2 a volume (four numbers) in advance. Single numbers, 75 cents. All drafts and money orders should be made payable to THE ANNALS OF MATHEMATICS.

PRESS OF THE NEW ERA PRINTING COMPANY, LANCASTER, PA.

DECEMBER, 1916

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

Stanford University Library
JAN 18 1917

EDITED BY

ORMOND STONE
L. P. EISENHART
OSWALD VEBLEN
PIERRE BOUTROUX
T. H. GRONWALL
J. H. M. WEDDERBURN

WITH THE COÖPERATION OF

J. W. ALEXANDER
R. D. CARMICHAEL
A. A. BENNETT
H. H. MITCHELL

PUBLISHED UNDER THE AUSPICES OF PRINCETON UNIVERSITY

SECOND SERIES, VOL. 18, NO. 2

LANCASTER, PA., AND PRINCETON, N. J.

CONTENTS

PAGE

The Numerical Factors of the Arithmetic Forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$. By TRACY A. PIERCE 53

A Problem in Geometry connected with the Analytic Continuation of a Power Series. By T. H. GRONWALL 65

On the Power Series for Log $(1 + z)$. By T. H. GRONWALL . . . 70

On the Convergence of Binet's Factorial Series for Log $\Gamma(s)$ and $\psi(s)$. By T. H. GRONWALL 74

Note on Cauchy's Integral Formula. By J. L. WALSH 79

On the Rational, Integral Invariants of Nilpotent Algebras. By OLIVE C. HAZLETT 81

On Trigonometric Series. By WILLIAM LEROY HART 99

Copies of the following memoir can be obtained by addressing THE ANNALS OF MATHEMATICS, Princeton, N. J.:

An Elementary Exposition of the Theory of the Gamma Function. By J. L. W. V. JENSEN. Authorized translation with additional notes by T. H. GRONWALL. 43 pages. Price 50 cents.

ANNALS OF MATHEMATICS

Published in September, December, March and June, at Lancaster, Pa. and Princeton, N. J., U. S. A.

Communications should be addressed to The Editors of the *Annals of Mathematics*, Princeton, N. J., U. S. A. Subscription price, $2 a volume (four numbers) in advance. Single numbers, 75 cents. All drafts and money orders should be made payable to THE ANNALS OF MATHEMATICS.

PRESS OF THE NEW ERA PRINTING COMPANY, LANCASTER, PA.

Stanford University Library
MAR 23 1917

MARCH, 1917

Please read the announcement on the inside of the front cover.

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

EDITED BY

ORMOND STONE
L. P. EISENHART
OSWALD VEBLEN
PIERRE BOUTROUX
T. H. GRONWALL
J. H. M. WEDDERBURN

WITH THE COÖPERATION OF

J. W. ALEXANDER
R. D. CARMICHAEL
A. A. BENNETT
H. H. MITCHELL

PUBLISHED UNDER THE AUSPICES OF PRINCETON UNIVERSITY

SECOND SERIES, VOL. 18, NO. 3

LANCASTER, PA., AND PRINCETON, N. J.

An agreement has been made between the Mathematical Association of America and the Annals of Mathematics in accordance with which the Association will contribute to the support of the Annals; the Annals will enlarge its volume by 100 pages which are to be devoted to expository and historical articles in so far as suitable material of this sort is available; and the subscription price to individual members of the Association will be one-half of the regular price. The regular subscription price of the Annals beginning with Volume 19 will be $3.00 a volume.

CONTENTS

PAGE

Symmetric Functions formed by Systems of Elements of a Finite Algebra and their Connection with Fermat's Quotient and Bernoulli's Numbers. By H. S. VANDIVER 105

The Generalized Lagrange Indeterminate Congruence for a Composite Ideal Modulus. By H. S. VANDIVER 115

On the Congruence $cx^\lambda + 1 = dy^\lambda$ in a Galois Field. By HOWARD H. MITCHELL 120

On the Geodesics and Geodesic Circles on a Developable Surface. By WILLIAM CASPAR GRAUSTEIN 132

Note on Representations of the Partial Sum of a Fourier's Series. By DUNHAM JACKSON 139

Acknowledgment. By FRANK IRWIN 146

Certain General Properties of Functions. By HENRY BLUMBERG . . 147

Copies of the following memoir can be obtained by addressing THE ANNALS OF MATHEMATICS, Princeton, N. J.:

An Elementary Exposition of the Theory of the Gamma Function. By J. L. W. V. JENSEN. Authorized translation with additional notes by T. H. GRONWALL. 43 pages. Price 50 cents.

ANNALS OF MATHEMATICS

Published in September, December, March and June, at Lancaster, Pa. and Princeton, N. J., U. S. A.

Communications should be addressed to The Editors of the *Annals of Mathematics*, Princeton, N. J., U. S. A. Subscription price, $2 a volume (four numbers) in advance. Single numbers, 75 cents. All drafts and money orders should be made payable to THE ANNALS OF MATHEMATICS.

PRESS OF THE NEW ERA PRINTING COMPANY, LANCASTER, PA.

UNIVERSITY LIBRARY

JUNE, 1917

Please read the announcement on the inside of the front cover.

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

EDITED BY

ORMOND STONE — PIERRE BOUTROUX
L. P. EISENHART — T. H. GRONWALL
OSWALD VEBLEN — J. H. M. WEDDERBURN

WITH THE COÖPERATION OF

J. W. ALEXANDER — A. A. BENNETT
R. D. CARMICHAEL — H. H. MITCHELL

PUBLISHED UNDER THE AUSPICES OF PRINCETON UNIVERSITY

SECOND SERIES, VOL. 18, NO. 4

LANCASTER, PA., AND PRINCETON, N. J.

An agreement has been made between the Mathematical Association of America and the Annals of Mathematics in accordance with which the Association will contribute to the support of the Annals; the Annals will enlarge its volume by 100 pages which are to be devoted to expository and historical articles in so far as suitable material of this sort is available; and the subscription price to individual members of the Association will be one-half of the regular price. The regular subscription price of the Annals beginning with Volume 19 will be $3.00 a volume.

Copies of the following memoirs can be obtained by addressing THE ANNALS OF MATHEMATICS, Princeton, N. J.:

An Elementary Exposition of the Theory of the Gamma Function. By J. L. W. V. JENSEN. Authorized translation with additional notes by T. H. GRONWALL. 43 pages. Price 50 cents.

Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers. By L. E. DICKSON. 27 pages. Price 25 cents.

CONTENTS

PAGE

Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers. By L. E. Dickson 161

The Modified Remainders Obtained in Finding the Highest Common Factor of Two Polynomials. By A. J. Pell and R. L. Gordon . 188

Nomograms of Adjustment. By L. I. Hewes 194

Closed Algebraic Correspondences. By Albert A. Bennett . . 200

The Intersections of a Straight Line and Hyperquadric. By J. L. Coolidge 209

The Relation between the Zeros of a Solution of a Linear Homogeneous Differential Equation and Those of its Derivatives. By William Benjamin Fite 214

Conjugate Planar Nets with Equal Invariants. By Luther Pfahler Eisenhart 221

ANNALS OF MATHEMATICS

Published in September, December, March and June, at Lancaster, Pa. and Princeton, N. J., U. S. A. Subscription price, $3 a volume (four numbers) in advance. Single numbers, $1.00. All drafts and money orders should be made payable to The Annals of Mathematics, Princeton, New Jersey.

Manuscripts and other communications should be addressed to Oswald Veblen, Princeton, N. J., U. S. A.

Authors receive gratis 50 reprints of each article, postage prepaid. Additional copies will be furnished at cost.

Press of The New Era Printing Company, Lancaster, Pa.